



International Journal of
**Infrastructure Research
and Management**

Vol. 10 (1), June 2022

ISSN 2811-3608
eISSN 2811-3705
PP 18094/04/2013(033449)

EDITOR-IN-CHIEF

Faridah Ibrahim, Prof., Dr.

ASSOCIATE EDITORS

Noor Saadah Zainal Abidin, Prof., Dr.
Karthiyaini Devarajoo, Assoc. Prof., Dr.
Manal Mohsen Abood, Assoc. Prof., Dr.
Golnoosh Manteghi, Dr.
Juliana Rosmdah Jaafar, Dr.
Siti Nur Aliaa Roslan, Sr Gs. Dr.

INTERNATIONAL ADVISORY BOARD

ANDI FAISAL BAKTI PROF. DR.

Universitas Pancasila, Jakarta, Indonesia

ANG PENG HWA PROF. DR.

Nanyang Technological University, Singapore

GARY RAWNSLEY PROF. DR.

University Aberystwyth, Wales, United Kingdom

IDERIS ZAKARIA PROF. DR.

Infrastructure University Kuala Lumpur, Malaysia

LATIFAH AMIN PROF. DR.

National University of Malaysia, Malaysia

MOHAMMAD ABDUL MANAN PROF. DR.

University Malaysia Sarawak, Malaysia

NAREN CHITTY A.M PROF. DR.

Macquarie University, Australia

OLIVER HAHN PROF. DR.

University of Passau, Germany

SAODAH WOK PROF. DR.

International Islamic University Malaysia, Malaysia

SITI MAZIHA MUSTAPHA PROF. DR.

Infrastructure University Kuala Lumpur, Malaysia

TIMOTHY GRAY PROF., AIA, LEED AP

Ball State University, U.S.A.

ENGLISH LANGUAGE EDITORS

Nur Widad Roslan, Dr.

Pavani Meganathan, Dr.

EDITORIAL ADVISOR

Annie Yap Ai Kin

EDITORIAL COORDINATOR

Nur Amalina Samusi

Published by
IKRAM Education Sdn. Bhd. *for*
INFRASTRUCTURE UNIVERSITY KUALA LUMPUR

Printed by
Printing Unit
KUMPULAN IKRAM SDN. BHD.

Disclaimer

The selection and presentation of materials and the opinions expressed are the sole responsibility of the author(s) concerned. Statements made by authors do not imply endorsement or agreement by the Chief Editor, the Editorial Board or Infrastructure University Kuala Lumpur (IUKL).

CONTENTS

No.	Title/Author	Page
1.	<i>Finite Element Analysis on the Steel Fiber-Reinforced Concrete Beams: A Systematic Review</i> Hou Zhicheng & Norhaiza Nordin	1
2.	<i>Sqlia Types and Techniques - A Systematic Analysis of Effective Performance Metrics for SQL Injection Vulnerability Mitigation Techniques</i> Aduragbemi David Ogundijo, Atiff Abdalla Mahmoud Arabi & Tadiwa Elisha Nyamasvisva	16
3.	<i>Technology Acceptance in Tourism Sector: A Systematic Review</i> Sulaiman Al Jahwari, Mohd. Dan Bin Jantan & Supriya Pulparambil	29
4.	<i>A Comprehensive SWOT Analysis for Zero Trust Network Security Model</i> Tadiwa Elisha Nyamasvisva & Atiff Abdalla Mahmoud Arabi	44
5.	<i>Women Leadership in Malaysian Creative Industry</i> Kartini Kamalul Ariffin & Faridah Ibrahim	54
6.	<i>Preservation of Architectural Model into 3 Dimensional Digital Form with the Methods of Photogrammetry</i> Adil Farizal Md Rashid, Rizal Husin & Md Pilus Md Noor	72
7.	<i>Zero Trust Security Implementation Considerations in Decentralised Network Resources for Institutions of Higher Learning</i> Atiff Abdalla Mahmoud Arabi, Tadiwa Elisha Nyamasvisva & Sangeetha Valloo	79

FINITE ELEMENT ANALYSIS ON THE STEEL FIBER-REINFORCED CONCRETE BEAMS: A SYSTEMATIC REVIEW

Hou Zhicheng and Norhaiza Nordin
Infrastructure University Kuala Lumpur, MALAYSIA

ABSTRACT

Steel fiber-reinforced concrete beams have been widely researched, including static mechanical performances, fatigue behaviors, prediction of capability and so on. It is widely accepted that numerical simulations are useful as they reduce more time, materials of casting and testing processes. This paper reviews the effect of finite element analysis on the steel fiber-reinforced concrete beams with commercial software ABAQUS and combines the results of the literature including FEA investigations. More than 150 papers were downloaded and only 8 papers from all the downloaded papers included contents of simulation specimen procedures with ABAQUS. Those papers were seriously compared between each other about what constitutive relations selected and details of defining other parameters in this presented work. What kind of material models in ABAQUS software was used more often and how to define the important parameters in recent study was discussed. Furthermore, this paper discusses of the two most important factors which are simulation accuracy and calculation efficiency about FEA and analyses the influence parameters based on the results of literatures. In brief, FEA simulation of SFRC beams with ABAQUS could be accomplished in good agreement between the experimental and numerical predict results and the discrepancies in general could be less than 10% with suitable data of other researcher's experiment, while the number will be limited to 5% with exact average data of experimental results based on the same group of material. It should be noted that ABAQUS software is valuable and enough accuracy for simulation of SFRC beams and already be general employed in project investigations in recent years based on literatures regarding SFRC beams.

Keywords:

Finite element analysis, steel fiber reinforced concrete, ABAQUS, accuracy, efficiency, review

INTRODUCTION

Steel fibers can maintain longer useful working life for the elements of reinforced concrete, increase the impact resistance and fatigue endurance. Alongside shrinkage reduction, they also distribute uniformly the stress taking by the SFRC, deduction of surface permeability, dusting and water can also be done. Steel fibers can increase through multi-direction (cross section), while conventional steel rebars only used to improve the concrete strength at single direction. Steel fibers always have been claimed that they are the best crack resistant materials for concrete, since they not only can prolong the crack to be happened and even cracking occurs, but also increase the initial crack strength. Many countries could produce qualified steel fibers around the world, such as HIC Corporation from Korea, Remix Steel Fiber Co. Ltd. from China, KIMMU (Group of Companies) from Malaysia. Steel fibers are needles of wire, deformed and cut to lengths, for reinforcement of mortar, concrete and some composite materials. Some fibers are cold drawn wire fibers with flatted or corrugated shapes. A. Bernard in California (1874) patented the designing of reinforcing concrete with the mean of the addition of steel splinter, since then, the long practice of inventing modern SFRC was began. According to a book (Steel fiber reinforced concrete) wrote by Maidl BR (1918), author patented an approach of modifying SFRC by long steel fibers in France, which could improve tensile strength of concrete. For recent six decades there have been investigated immense research projects devoted to the application of steel fibers and mechanical properties of SFRC. Nowadays, SFRC have become the third important concrete based on structural materials beside concrete reinforced by steel meshes and traditionally reinforced concrete (by stirrups and rods) (Katzner & Domski, 2012). Folino et al. (2020)

analysed the mechanical and failure behaviors of full-scale reinforced concrete beams reinforced with SFRC in their research. As predicted, it was realised that steel fibers contribute to increase the structural integrity in post-peak behaviour, both in structural and small beams. Yoo et al. (2017) have investigated the possibility of excluding the minimum shear reinforcement in reinforced sustainable high-strength concrete beams by addition of 0.75% (by volume) of steel fibers. Their results clearly demonstrated that addition of steel fibers in higher concrete beams would increase the performances of the beams which were identical to conclusions of other researchers (Mertol et al., 2015).

Abaqus company was set up in 1978 by Dr. David et al., since 2014, the headquarters of the company were located in Johnston, Rhode Island, United States. It's important product ABAQUS is a software used for both the simulation and analysis of mechanical assemblies and components (pre-processing) and visualizing the calculation results. Abaqus was originally designed to deal with non-linear physical behaviors, therefore, the package includes a large-scale range of material models such as hyperelastic (soft tissue) and elastomeric (rubberlike) material capabilities. The Abaqus Unified FEA product software offers complete and powerful solutions for both ordinary and sophisticated engineering issues covering an extensive spectrum of industrial applications. First-in-class companies are making use of Abaqus Unified FEA to consolidate their tools and processes, reduce costs and inefficiencies, and obtain a competitive advantage.

LITERATURE REVIEW

Research Objective and Scope of Study

Experimental study of size effects and different parameters of SFRC beams need to so many materials as well as labors since a large number of dimensions of similar elements will be casted to get the mechanical performances. For such objective, the cost-effective numerical simulations always were carried out in recent researches of SFRC beams.

A systematic approach was taken in this paper to investigate the finite element analysis on the steel fiber-reinforced concrete beams. The idea of numerical simulations with ABAQUS was highlighted in the SFRC beam investigations and industrial products fields in this paper. In the meantime, what kind of material models in ABAQUS software was used more often in recent study was also discussed. Therefore, how to define the important parameters such as the dilation angle, the viscosity parameter and so on in ABAQUS was presented further. Later, simulation accuracy and calculation efficiency, the most concerning factors about FEA with commercial software were compared between different study based on exact data from review papers. Finally, this paper concluded that FEA simulation of SFRC beams with ABAQUS could be accomplished in good agreement between the experimental and numerical predict results.

Review Methodology

This review about the Finite element analysis on the steel fiber-reinforced concrete beams began with the collection and assessment of relevant literatures published in recent decades. For papers collection, famous ScienceDirect and EThOS websites were utilized and updated up to March 2022. The keyword search included "steel fiber reinforced concrete beams" and then title (and abstract) screened. Moreover, other FEA software, for example, ANSYS and DIANA programs were introduced and employed in papers less than that with ABAQUS especially in papers published in recent years. Those papers were seriously compared between each other about what constitutive relations selected and details of defining other parameters for this presented work.

In the progress of comparing, first of all, all papers included in this paper were divided into different groups. The three main categories were: "static behaviors of SFRC beams", "dynamic

behaviour of SFRC beams” and “fire resistance of SFRC beams”. Every category of papers was simulated to different load of engineering, for an example, “static behaviors” included 3 or 4 point bending test, “dynamic behavior” included low-velocity impact loading test and fatigue behavior test. However, for “fire resistance behavior” category, just one paper (Liu et al. 2018) was found which presented fire load condition of engineering. Most papers discussed in this paper, their authors have not only carried out specimen test, but also calculated the SFRC beams with ABAQUS at the same time. And all their FEA results were very close with their experimental results. Therefore, based on those research of authors, the simulation with ABAQUS software was reliability clearly and strongly. The research process and methodology were shown in Fig.1.

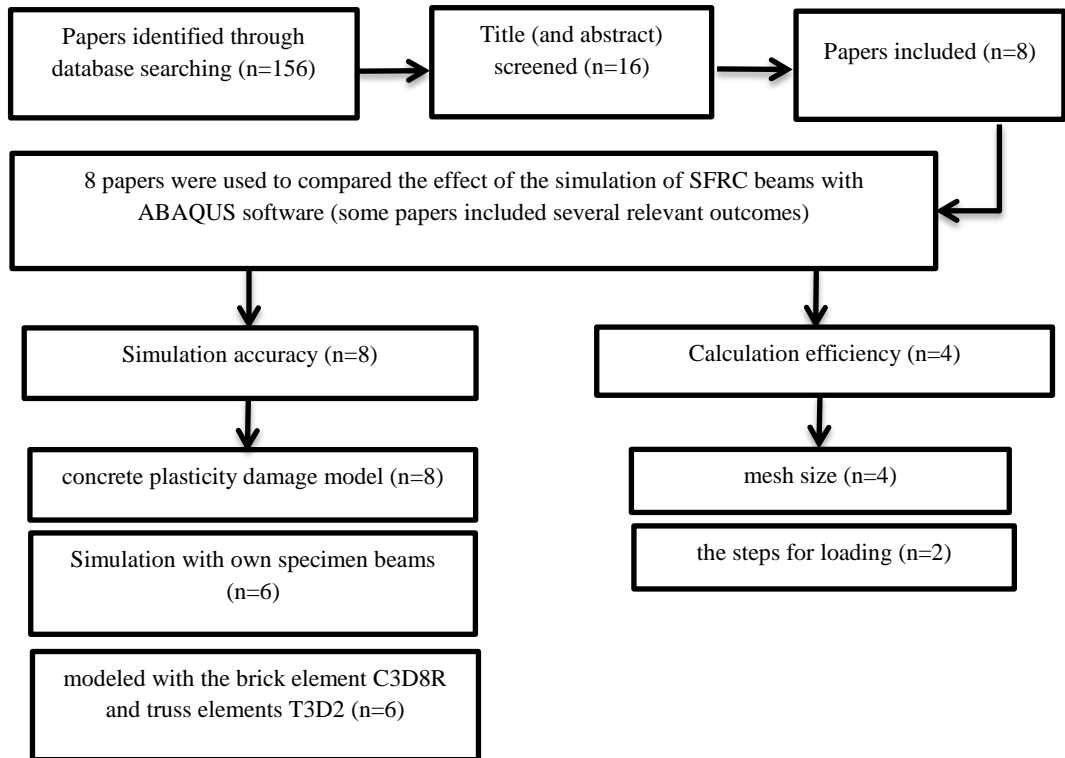


Figure 1: Flow chart of the research process and results.

REVIEW RESULTS

Finite Element Analysis of Static Behaviors of SFRC Beams

Hamoda et al. (2019) investigated numerically and experimentally behaviors of steel-I beam with or without high strength bolted connectors embedded in normal/Steel Fiber-Reinforced Concrete with the finite element package ABAQUS. In their FEA, all constitutive materials including SFRC, NC, steel I-beam, and internal steel reinforcements were created using suitable elements available in the Abaqus software. Furthermore, appropriate contact interactions, meshing properties and boundary conditions based on the performed push-out tests were established. And they employed concrete damage plasticity model to present the inelastic behaviors for both SFRC and NC (see Fig.2).

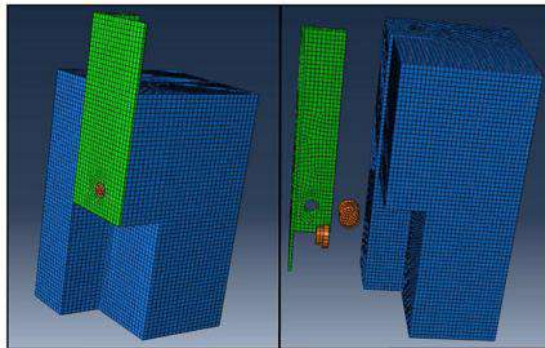


Figure 2: 3D Finite Element Model (Quarter of Specimen) (Hamoda et al. ,2019)

They identified the NC material stress-strain behaviors according to compressive and splitting tests performed experimentally (see Fig.3). The integrity of FEA results was carefully compared and verified against those experimental results with variation about 8% that can be enough valuable for investigating composite section with short demountable bolted connectors (see Fig.4).

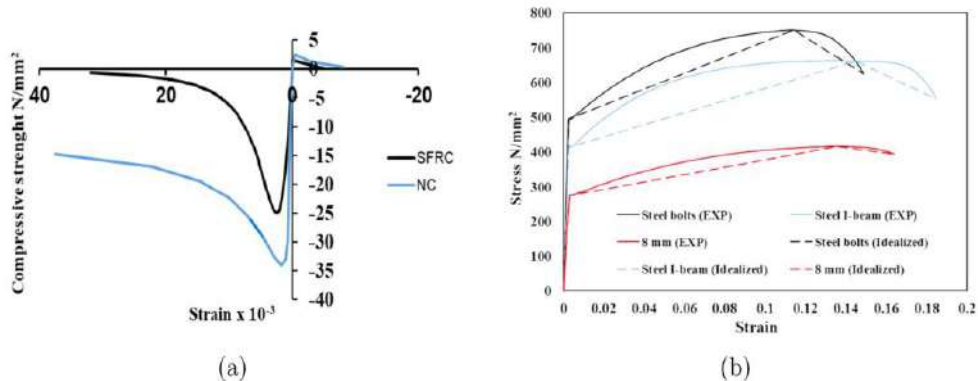


Figure 3: Material Stress-strain Laws Adopted in Finite Element Modeling;(a) Concrete (b) Real and Idealized Uniaxial Stress Strain Relation for Steel Elements (Hamoda et al. ,2019)

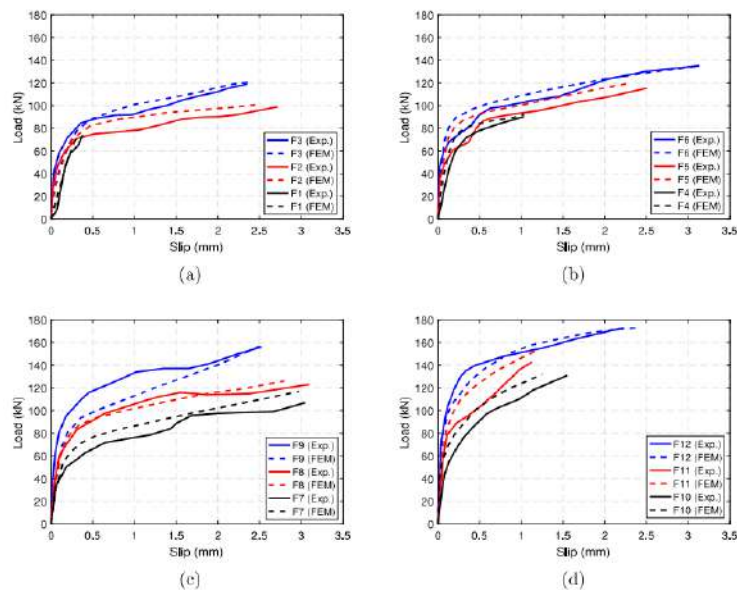


Figure 4: Experimental Versus Finite Element Load-slip Curves for Specimens Made of SFRC (Hamoda et al. ,2019)

Their experiment clearly demonstrated that investigating mechanical performances of some elements with the finite element package ABAQUS is useful and it could be accurately agreement with practical samples. Their process of research in developing nonlinear 3D-FEA model with the finite element package ABAQUS was perfect and could be example in future research about investigation of SFRC beams.

Experimental researches of various SFRC beams were expensive because of a wide range of dimensions of similar beams needed to be casted and tested to gain a full-size effect law. Therefore, researchers often simulated the experimental elements with the versatile, cost-effective numerical models. In research of size effects of Ultra High Performance Steel Fiber Reinforced Concrete (UHPC) beams from Mahmud et al. (2013) as in Fig.5, they modeled nonlinear finite element SFRC beams using the concrete damage plasticity model in ABAQUS too. They assumed that steel fibers were evenly distributed in the matrix and the UHPC was thus simulated as a homogeneous material.

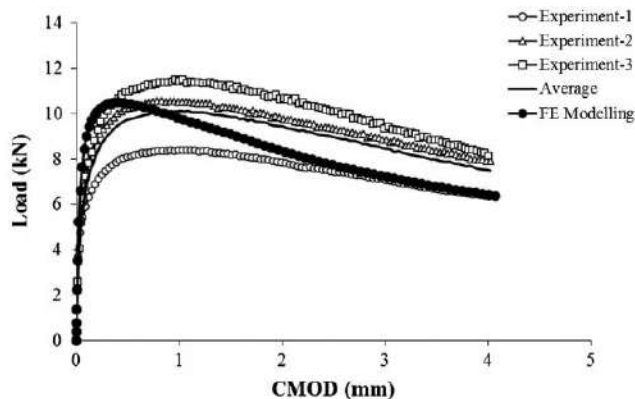


Figure 5: Load-CMOD Curves for Beams with $d=60\text{mm}$ (Mahmud et al. ,2013)

They ran the command *CONCRETE TENSION STEFFEINIGN, TYPE=DISPLACEMENT in beams simulation process with ABAQUS for implementing equivalent stress-crack opening displacement (COD) curves. Meanwhile, the compressive strengths of SFRC were modeled with running the command*CONCRETE COMPRESSION HARDENING, TYPE=STRAIN. They noted that the mechanical properties of samples captured from experiments include elastic parts but inelastic quantities were established for the simulation with ABAQUS so transformation was needed. All the beams were modelled with reduced-integration 4-noded plain stress elements (CPS4R).

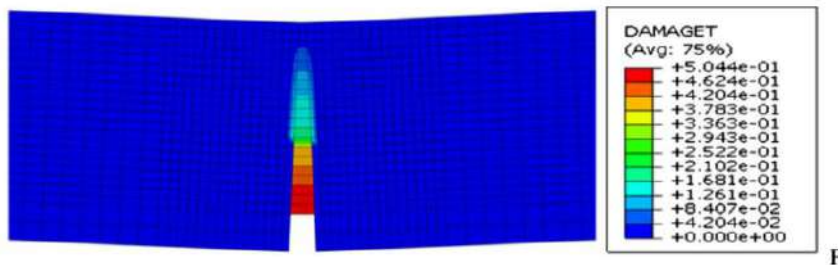


Figure 6: A Deformed Mesh with Damage Contours (Mahmud et al. ,2013)

They compared the three load-CMOD and average curves obtained from their bending tests with the CDP-based numerical results in Fig.4 for beam with $d=60\text{mm}$ as an example. Overall good agreements between the experimental and numerical results can be observed. They estimated that the discrepancy maybe attribute to the input pre-load 2 kN which was too close to their peak load of beam about 2.5-3.5 kN. They showed the deformed mesh with damage contours in Fig.6, and their analysis demonstrated that the CDP-based finite element models could predict the bending capacities of the UHPFRC beams with considerable accuracy and therefore parametric studies can further be carried out for size effect analysis (see Fig.7). According to the research of Mahmud et al. (2013), it was proved that a full-size effect law about the UHPFRC beams could be predicted with ABAQUS and pre-load to sample need to be designed carefully in future research.

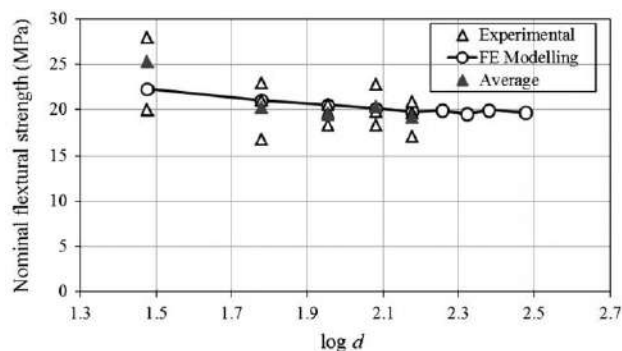


Figure 7: Size Effect on the Nominal Flexural Strength of UHPFRC Beams (Mahmud et al. ,2013)

Simwanda et al. (2021) have validated nine beams which were conducted by other three researchers by comparing experimental load-deflection capacity and FE predicted load-deflection capacity with ABAQUS software in their study. It was indicated that there was a good agreement in terms of peak load, initial stiffness and corresponding displacement. Shewalul et al. (2021) have modeled a continuous beam with two spans using the FEA software ABAQUS. They calculated the amount of moment redistribution with FEA and verified the results based on experimental tests at

Stellenbosch University. Their FEA models and experimental specimen provided almost similar results with a nearly similar mid span response.

Finite element analysis of dynamic behaviour of SFRC beams

Murthy et al. (2018) created a finite element model to predict the number of cycles to failure and load-deflection behaviour of the RC beams strengthened with ultra-high performance fiber reinforced concrete. The data of compressive stress and strain were quoted from experiments of Mier et al. Further, the constitutive of post cracking relationships for materials were obtained from the works of Almusallam TH et al. They employed the concrete plastic damage model to present the nonlinear behaviour of SFRC. The concrete beam and steel rebars were modeled with elements mentioned earlier. The FE model and typical assembly were shown as Fig.8.

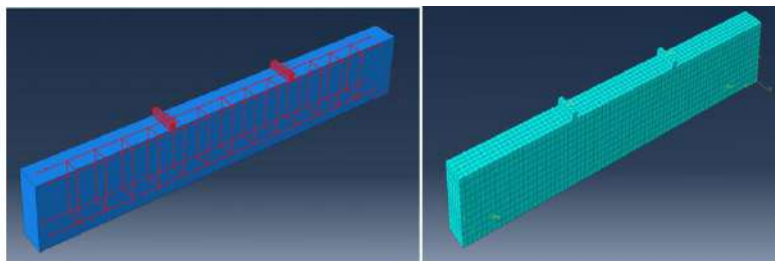


Figure 8: Typical Assembly and FE Model (Murthy et al. ,2018)

Their beams were analyzed with direct cyclic loading with FEA ABAQUS software. The frequency of loading based on the experiments was simulated as periodic amplitude as depicted in Fig.8.

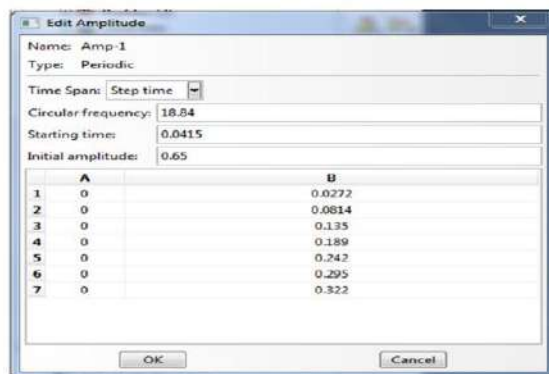


Figure 9: Cyclic Load data input in ABAQUS (Murthy et al. ,2018)

Furthermore, they compared the predicted load-deflection behaviour and the number of cycles to failure with the average experimental results. Fig.9 and Fig.10 clearly demonstrate the parts of results, there was very good agreement between the FEA results and practical observations. Furthermore, the maximum difference from comparison was less than 10%. However, the discrepancy from other researchers was 5% more or less and the more accurately results was because of simulation with data of constitutive relationship obtained from practical experiments carried out by researchers themselves. Therefore, it is widely accepted that simulation SFRC beams in FEA with the data from

the same project is best choice and could make the numerical results as closely as possible to the experimental.

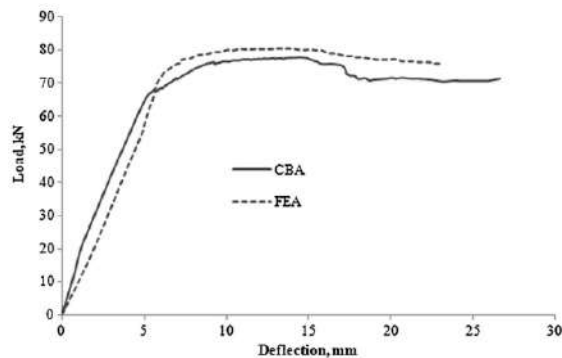


Figure 10: Predicted Load-Deflection Curve of Control RC Beam Compared with Average Experimental Curve (Murthy et al. ,2018)

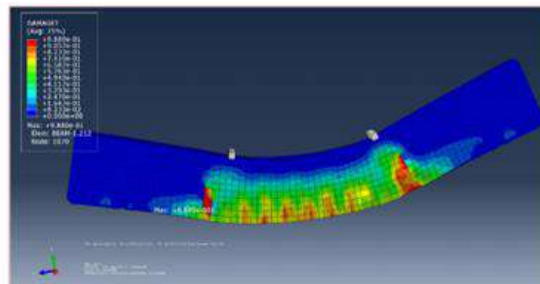


Figure 11: Flexural Damage Pattern for Typical Retrofitted Beam (Murthy et al. ,2018)

Gao et al., (2021) have ever considered fiber clustering in the concrete damaged plasticity model in ABAQUS and simulated the crack patterns of SFRC beam. Their FEA results agreed well with the experimental results, and they suggested that ABAQUS software could be used to investigate the fiber clustering effects in other SFRC structures. Mohsin (2012) had modeled a lot of SFRC beams with ABAQUS software in research of PHD period and calibrated them with experimental results from Campione et al., (2003, 2006) and Mangiavillano (2008). The FEA models yielded the most satisfactory agreement with experimental data.

Finite Element Analysis of Fire Resistance of SFRC Beams

Jin et al. (2018) carried out the experiment of fire resistance of SFRC beams after low-velocity impact loading. In their research, they established a finite element numerical model which considering the effects of high temperature and strain rate. Similar with the aforementioned work, they described the behaviour of SFRC with the concrete plasticity damage model which proposed by Lubliner et al. (1989) and later updated by Lee and Fenves (1998). This model was widely employed for the simulation of static and dynamic behaviors of SFRC. They took into account of the mechanical properties of SFRC which altered by steel fibers and utilized the data from their own experimental tests. About the basic material parameters, such as Young's modulus, strength and strain at peak stress were inputted in model according to Chinese code. It should be noted that the model was meshed by eight-node solid element except that steel rebar was meshed by two-node wire element. At last, the

model was meshed to total number of degrees of freedom up to 800000 and the mesh sizes of SFRC and steel rebar were 10mm while other parts of model was meshed to elements of size 30mm which could improve calculation efficiency. The setup of experiment was depicted as Fig.11. The numerical results were presented after simulating two steps which were exactly as same as the practical experiments. The parts of FEA results and comparison conclusions were displayed in Fig.12 and Fig.13.

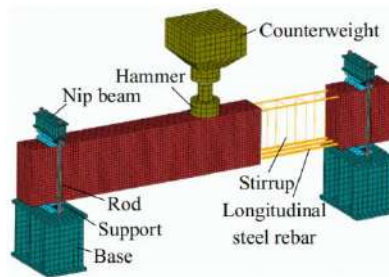


Figure 12: Finite Element Computational Model of the Beam (Jin et al. ,2018)

Based on those results of pictures, it was obviously demonstrated that slight discrepancies were no chance to eliminated totally and the reasons of that already been explained logically by the researchers in their analysis procedures. However, it still can be proved that the FEA method was effective to simulate the main behaviour of SFRC beams exposed to both impact loading and fire.

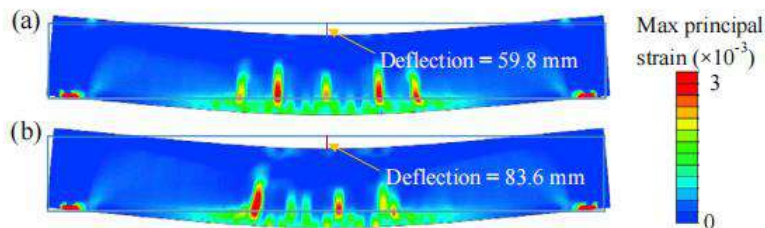


Figure 13: The Effect of Impact-induced-Damage on Fire Deformation of SFRC Beam B-2. (a)Without impact loading; (b) After Impact loading (Jin et al. ,2018)

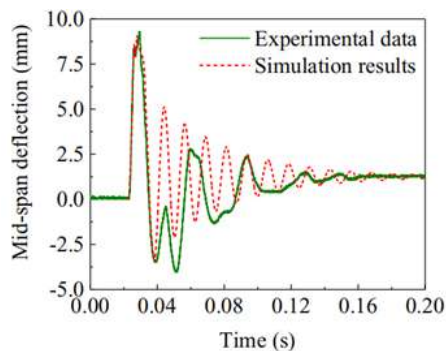


Figure 14: Comparison Between the simulated Mid-span Deflection Time Histories with the Experimental Ones for B-2 (Jin et al. ,2018)

CONSTITUTIVE MODELS FOR SFRC AND MATERIAL MODELS IN ABAQUS SOFTWARE

Constitutive Models for SFRC

Over the past few decades, many constitutive models for SFRC have been proposed based on practical experiments and theory calculation. To get the post behaviors of SFRC, a number of compressive and flexural samples were tested by researchers. RILEM TC 162-TDF Recommendations (2000) proposed stress-strain relations for SFRC. The compressive strength was subsumed to be improved than that of plain concrete. More recent works for stress-strain relations were done later, RILEM TC 162-TDF (2003) updated the residual flexural strength of SFRC with the following crack mouth opening displacement or midspan deflection values. Moreover, Barros and Figueiras (2001) and Tlemat et al. (2006) had proposed SFRC model separately. Researchers ran their experimental data obtained from cylinders and dog-bone specimens in general as the stress-strain relationship in FEA simulations which were not in the same scales with that of curves they depended (Jin et al., 2018 & Gao et al., 2021).

Material models in ABAQUS software

The concrete damage plasticity model in ABAQUS was used in most study, assuming steel fibers were uniformly distributed in the matrix and then the SFRC was modeled as a kind of homogeneous material (Jin et al., 2018 & Gao et al., 2021). There are about five other parameters needed to be defined in SFRC model basically: in most cases, the dilation angle in degrees is 33, the flow potential eccentricity is 0.1, the ration of initial equibiaxial compressive yield stress to initial uniaxial compressive yield stress is 1.16, the viscosity parameter is 0.66 and the ration of the second stress invariant on the tensile meridian to that on the compressive meridian is 0 (Mahmud et al., 2013). These values were insignificant to the results of simulation based on opinion from Mahmud et al. (2013) and Wang et al (2017). Further, the SFRC or the beams were modeled with the brick element C3D8R (Cube Three Dimensional eight-node Reduced integration) in many investigations and the reinforced steel rebars were generally modeled with three dimensional truss elements (T3D2) which having three translational degrees of freedom at each node (Gao et al., 2021).

RESULTS AND DISCUSSION

Simulation Accuracy

It is obviously that the most concerning factors about FEA with commercial software are simulation accuracy and calculation efficiency. It is no chance to make FEA simulation absolutely equal to practical experimental results as even performances captured from two same beams with total same designation cannot be the same. The slight discrepancy may be from the assumption of material homogeneity, different properties and loadings and so on (Mahmud et al., 2013).

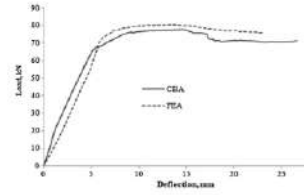
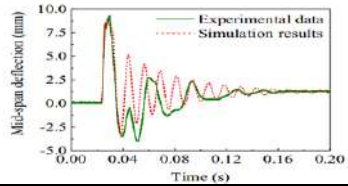
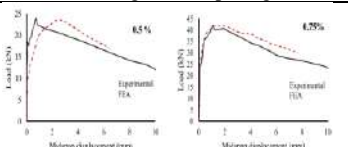
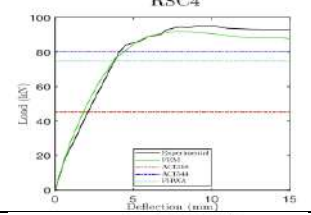
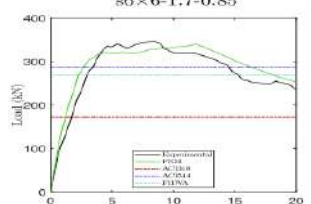
No.	investigators	Type of study	Details of database							Results																																								
			Dimensions (mm ³)	No. of specimens	Type of concrete	Fiber type	variable	L _f (mm)	V _f (%) or (kg)	P _{cr} error [kN]	Max. load error [kN]																																							
[1]	Hamoda et al.	ABAQUS	200×200×200mm ³	12	NC	/	/	/	/	-1.1%~5.4%	-8.6%~4.5%																																							
				12	SFRC	hook-end	/	/	/	-4.4%~7.1%	-2.6%~9.3%																																							
[2]	Murthy et al.	ABAQUS	200×100×1500mm ³	1	NSC	/	loading	/	/	 <p>Fig. 15. Predicted load - deflection curve of control RC beam compared with average experimental curve.</p>																																								
				3	UHPFRC	Brass-coated	loading	13m	2%																																									
[3]	Mohsin	ABAQUS	150×150×550mm ³ (monotonic loading)	2	SFRC	hook-end	V _f (%)	30m	0%,1%	<table border="1"> <thead> <tr> <th>Beam</th> <th>P_y (kN)</th> <th>δ_y (mm)</th> <th>P_u (kN)</th> <th>δ_u (mm)</th> <th>P_{max} (kN)</th> <th>δ_{max} (mm)</th> <th>μ = δ_u/δ_y</th> </tr> </thead> <tbody> <tr> <td>Experimental (VF=0%)</td> <td>100.0</td> <td>2.15</td> <td>127.4</td> <td>13.74</td> <td>127.4</td> <td>13.74</td> <td>6.39</td> </tr> <tr> <td>FE analysis (VF=0%)</td> <td>95.41</td> <td>1.6</td> <td>115.0</td> <td>11.77</td> <td>120.48</td> <td>5.80</td> <td>7.37</td> </tr> <tr> <td>Experimental (VF=1%)</td> <td>122.5</td> <td>2.15</td> <td>125.1</td> <td>19.3</td> <td>138.8</td> <td>10</td> <td>8.98</td> </tr> <tr> <td>FE analysis (VF=1%)</td> <td>117.95</td> <td>1.6</td> <td>132.2</td> <td>18.1</td> <td>136.36</td> <td>5.81</td> <td>11.31</td> </tr> </tbody> </table>	Beam	P _y (kN)	δ _y (mm)	P _u (kN)	δ _u (mm)	P _{max} (kN)	δ _{max} (mm)	μ = δ _u /δ _y	Experimental (VF=0%)	100.0	2.15	127.4	13.74	127.4	13.74	6.39	FE analysis (VF=0%)	95.41	1.6	115.0	11.77	120.48	5.80	7.37	Experimental (VF=1%)	122.5	2.15	125.1	19.3	138.8	10	8.98	FE analysis (VF=1%)	117.95	1.6	132.2	18.1	136.36	5.81	11.31
			Beam	P _y (kN)	δ _y (mm)	P _u (kN)	δ _u (mm)	P _{max} (kN)	δ _{max} (mm)	μ = δ _u /δ _y																																								
Experimental (VF=0%)	100.0	2.15	127.4	13.74	127.4	13.74	6.39																																											
FE analysis (VF=0%)	95.41	1.6	115.0	11.77	120.48	5.80	7.37																																											
Experimental (VF=1%)	122.5	2.15	125.1	19.3	138.8	10	8.98																																											
FE analysis (VF=1%)	117.95	1.6	132.2	18.1	136.36	5.81	11.31																																											
150×150×550mm ³ (reversed cyclic loading)	2	SFRC	hook-end	V _f (%)	30m	0%,1%	<table border="1"> <thead> <tr> <th>Column</th> <th>N_c (kN)</th> <th>P_y (kN)</th> <th>δ_y (mm)</th> <th>P_u (kN)</th> <th>δ_u (mm)</th> <th>P_{max} (kN)</th> <th>δ_{max} (mm)</th> <th>μ = δ_u/δ_y</th> </tr> </thead> <tbody> <tr> <td>Experimental</td> <td>2.0</td> <td>101.8</td> <td>2.7</td> <td>120.0</td> <td>9.41</td> <td>120.0</td> <td>9.41</td> <td>3.48</td> </tr> <tr> <td>FE analysis</td> <td>1.67</td> <td>114.6</td> <td>2.7</td> <td>126.71</td> <td>9.17</td> <td>126.71</td> <td>9.17</td> <td>3.40</td> </tr> </tbody> </table>	Column	N _c (kN)	P _y (kN)	δ _y (mm)	P _u (kN)	δ _u (mm)	P _{max} (kN)	δ _{max} (mm)	μ = δ _u /δ _y	Experimental	2.0	101.8	2.7	120.0	9.41	120.0	9.41	3.48	FE analysis	1.67	114.6	2.7	126.71	9.17	126.71	9.17	3.40																
Column	N _c (kN)	P _y (kN)	δ _y (mm)	P _u (kN)	δ _u (mm)	P _{max} (kN)	δ _{max} (mm)	μ = δ _u /δ _y																																										
Experimental	2.0	101.8	2.7	120.0	9.41	120.0	9.41	3.48																																										
FE analysis	1.67	114.6	2.7	126.71	9.17	126.71	9.17	3.40																																										

Table 1: Summary of previous experiments on SFRC beams with FEA and Formula

Table 1 (continued-1)

No.	Investigators	Type of study	Details of database							Results	
			Dimensions (mm ³)	No. of specimen	Type of concrete	Fiber type	Variable	L _f (mm)	V _f (%) or (kg)	Average P _u [kN]	Max. load error [kN]
[4]	Mahmud et al.	ABAQUS	30×150×500mm ³	3	UHPRC	straight	d	13	2.0%	3.17	11.8%
			60×150×500mm ³	3	UHPRC	straight		13	2.0%	10.13	3.6%
			90×150×500mm ³	3	UHPRC	straight		13	2.0%	22.03	4.7%
			120×150×500mm ³	3	UHPRC	straight		13	2.0%	40.73	1.2%
			150×150×500mm ³	3	UHPRC	straight		13	2.0%	61.75	2.7%
[5]	Jin et al.	ABAQUS	200×400×2800mm ³	1	SFRC	hook-end	Impact loading and temperatures	30	2%		
[6]	Gao et al.	ABAQUS	120×200×1200mm ³	8	SFRC	hook-end	V _f loading	35	0% to 2%	agree well with the experimental results in terms of the crack patterns, crack numbers, and average crack spacing	
[7]	Shewalul et al.	ABAQUS	150×250×3100mm ³	1	SFRC	/	V _f	/	0% to 1.5%		
[8]	Simwanda et al.	ABAQUS	Database from Kahanji	3	UHPRC	Various shape	V _f	l _f /d _f =6.5	1%, 2%, 4%		
			Database from Shafieifar et al.	3					2%		

			Database from Yang et al.	3			A_s		2%	
--	--	--	---------------------------	---	--	--	-------	--	----	--

There are some important aspects which should influence the simulation accuracy in FEA with ABAQUS software, such as constitutive relationship to SFRC, selecting of mesh elements to material and other concerning parameters. According to works aforementioned, the concrete plasticity damage model was employed mostly in recent years and which could make FEA results with ABAQUS more accurate than other models (Jin et al., 2018 & Gao et al., 2021). For better results that are as close as possible to practical experimental results, the data from practical experiments which are carried out with beams needed to predict is better than that from other experiments. The average discrepancy could be less than 5% with data belongs to same experiment while the number maybe up to 10% with other data (Mahmud et al., 2013, Murthy et al., 2018 and Jin et al., 2018). Furthermore, more accurate simulation for SFRC beams, in general SFRC are modelled with the brick element C3D8R and steel rebars are model with three dimensional truss elements (T3D2). And the conventional steel reinforcement was embedded in the matrix using the embedded interaction property (Simwanda et al., 2021, Ahmed et al., 2019 and Gao et al., 2021). About the boundary conditions, they have mentioned that rigid steel plates were tied on the support and loading points (Gao et al., 2021). The side supports and mid span support were restricted in some direction based on structural behaviors (Yohannes et al., 2021). As for Young's modulus and the Poisson's ratio were usually defined as 45 GPa and 0.22, which were based on current experiment or the other as it is insignificantly for simulation accuracy based on the literature mentioned above (Mahmud et al., 2013).

Calculation efficiency

Calculation efficiency is concerned by many researchers since it decides how long will the simulation process last. For an identical model, standard of calculation efficiency mainly depends on the number of elements model meshed. It is obviously that the more elements the more accuracy, however, the less efficiency or the longer time the simulation process needs for an identical scale model simulation. Therefore, it should be noted that this question about the number of elements is a balance issue in essence. In general, the parts of model on which stress varies significantly were meshed smaller elements while other parts no need to mesh so small for better calculation efficiency. For investigation of Jin et al. (2018), a mesh size of 10mm was adopted for SFRC and steel rebars while 30mm for other parts. Their choice of element number made the calculation process last 12h which was an acceptable time of simulation while their numerical simulation was enough effective. Mahmud et al. (2013) meshed their beam with $d=60\text{mm}$ model, and 5mm, 2.5mm and 1.25mm mesh sizes were selected near the beam center. It was found that the latter two sizes led to virtually identical results. Therefore, their other models were all based on the mesh size 2.5mm and successfully predicted the mechanical performances of SFRC beams with enough accuracy. Moreover, the decision of the steps for loading is as important as the number of elements for the purpose of calculation efficiency and the rules of two aspects are the same basically. This article will not discuss more about it.

CONCLUSIONS

Recent development in FEA simulation of SFRC beams with commercial software ABAQUS have been reviewed. The following concluding remarks are drawn.

1. FEA simulation of SFRC beams with ABAQUS could be accomplished in good agreement between the experimental and numerical predict results.

2. In FEA simulation of SFRC beams with ABAQUS, the concrete plasticity damage model was adopted mostly which was proved to be more accuracy than other concrete models in recent investigations.

3. For identical FEA simulation model with ABAQUS, there is a suitable size of element on parts of model considering calculation efficiency and too small elements are not meaningful to valuable simulation accuracy.

4. Simulation results of SFRC beams with ABAQUS, the discrepancies in general could be less than 10% with suitable data of other researcher's experiment while the number will be limited to 5% with exact average data of experimental results based on the same group of material.

AUTHOR BIOGRAPHY

Hou Zhicheng, a Postgraduate student in Doctor of Philosophy in Civil Engineering (by Research) in Faculty of Engineering and Technology Infrastructure, Infrastructure University Kuala Lumpur. He comes from China, was supervised by Norhaiza Nordin. *Email: 836715392@qq.com*

Norhaiza Nordin, PhD. Head of Post Graduate Program (HOPP), Senior Lecturer, Civil Engineering & Construction Division, Faculty of Engineering, Science and Technology, Infrastructure University Kuala Lumpur. *Email: norhaiza@iukl.edu.my*

ACKNOWLEDGEMENT

The authors would like to acknowledge all researchers included in this review paper whose previous researches contributed immensely to the accomplishment of the present research. This research was supported by Infrastructure University Kuala Lumpur and Faculty of Engineering, Science and Technology.

REFERENCES

- Ahmed Hamoda, Mohamed Emara, Walid Mansour (2019). Behavior of steel I-beam embedded in normal and steel fiber reinforced concrete incorporating demountable bolted connectors. *Composites: Part B*, 174 (2019),106996.
- A. Ramachandra Murthy, B.L. Karihalooob, P. Vindhya Ranic, D. Shanmuga Priya (2018). Fatigue behaviour of damaged RC beams strengthened with ultrahigh performance fibre reinforced concrete. *International Journal of Fatigue*, 116 (2018), 659-668.
- Danying Gao, Zhiqiang Gu, Congjie Wei, Chenglin Wu, Yuyang Pang (2021). Effects of fiber clustering on fatigue behavior of steel fiber reinforced concrete beams. *Construction and Building Materials*, 301 (2021), 124074.
- Goran H. Mahmud, Zhenjun Yang, Aram M.T. Hassan (2013). Experimental and numerical studies of size effects of Ultra High Performance Steel Fiber Reinforced Concrete (UHPFRC) beams. *Construction and Building Materials*, 48 (2013),1027–1034.

- Liu Jin, Renbo Zhang, Guoqin Dou, Xiuli Du (2018). Fire resistance of steel fiber reinforced concrete beams after low-velocity impact loading. *Fire Safety Journal*, 98 (2018): 24–37.
- L. Simwanda , N. De Koker, C. Viljoen (2018). Structural reliability of ultra high-performance fibre reinforced concrete beams in flexure. *Engineering Structures*, 244 (2021),112767.
- Sharifah Maszura Binti Syed Mohsin (2012). *Behaviour of fibre-reinforced concrete structures under seismic loading*. London: Imperial College, London.
- Yohannes Werkina Shewalul (2021). Numerical and FEA investigation of sectional capacity and moment redistribution behavior of steel fiber reinforced concrete (SFRC) beam. *Heliyon*, 7 (2021), e07354.

SQLIA TYPES AND TECHNIQUES - A SYSTEMATIC ANALYSIS OF EFFECTIVE PERFORMANCE METRICS FOR SQL INJECTION VULNERABILITY MITIGATION TECHNIQUES

Aduragbemi David Ogundijo, Atiff Abdalla Mahmoud Arabi and Tadiwa Elisha Nyamasvisva
Infrastructure University Kuala Lumpur, MALAYSIA

ABSTRACT

According to Open Web Application Security Project (OWASP), an online community that produces well-researched reports in the field of web application security, Structured Query Language (SQL) injection remains in the top three most common input vulnerability in applications due to the progression from static to dynamic web pages leading to increased database use in web applications. SQL injection vulnerabilities is prevalent in web and mobile applications because of common unsafe coding practices. A successful SQL injection attack poses a significant risk to the database, application, and web server as a whole. In this article, the authors have examined approaches for preventing SQL injection attacks and categorize SQL injection attacks based on the methods used to exploit SQL vulnerabilities. In terms of preventing all forms of SQL injection attacks, the discussed approach appears to be acceptable. This review paper presents a systematic review of the mitigation steps which include reconnaissance, enumeration, and extraction of data. Also discussed are types of injection attacks, some alternative procedures for mitigating SQL attacks and performance metrics for measuring the effectiveness of SQL injection mitigation techniques.

Keywords:

Injection Attacks, Mitigation Techniques, Detection Mechanisms, Vulnerability Exploitation, Anomaly Detection, Tautology, SQLIA

INTRODUCTION

The data management (model), display or front-end tiers (view) and application processing(controller) also called Model-View-Controller (MVC), are conceptually separated in today's web applications, and are based on an n-tier architecture. Instead of rewriting entire programs, developers now just need to add or alter a single layer as needed, making design and maintenance easier. (Al-Ahmad et al., 2014; Aniche et al., 2018; Paolone et al., 2021)

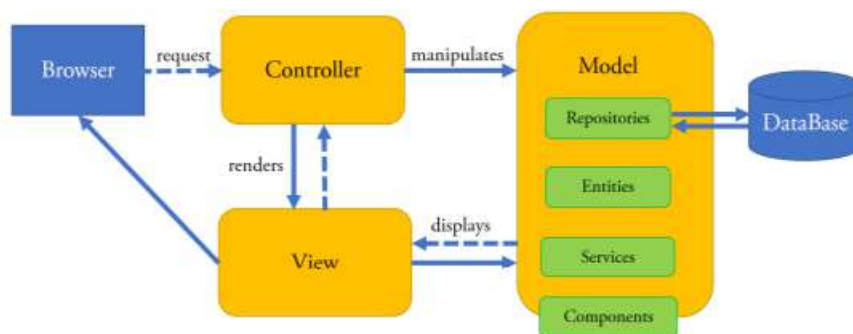


Figure 1. MVC Architecture as illustrated in (Aniche et al., 2018; Paolone et al., 2021)

The model or data management layer consists of a database server that stores and retrieves sensitive information about the application and its users. The database data is frequently used for user

authentication, storing records and their relationships, and presenting the data on a dynamically generated web page. Application Programming Interfaces (APIs) such as Open Database Connectivity (ODBC) and Java Database Connectivity are used to link the web application to the database management system (JDBC). Connection to the database servers are established and SQL queries are run using the built-in objects and methods. The SQL query processor receives the queries and executes them. The application server receives the results of the queries. The application server examines the returned data and makes a judgment, after which the data is rendered in the dynamic web page by the browser. User-supplied parameters are frequently included in the query that is sent to the database server for execution. The user-supplied input parameters may or may not be reliable. The query processor will, of course, run the query and deliver the result to the browser for display to user regardless of the query's type. The query, however, might still include malicious code or be logically wrong.

Attackers can inject malicious code into the input parameter as a result of the MVC design. If the code fails to appropriately isolate programme instructions from user data, the adversary may be able to do malicious input. By modifying the SQL query, the attacker can extract confidential information from the database and obtain complete control of the database and database server. The term "SQL injection attack" is used by hackers to describe this type of web application attack. The attack's main benefit is that it uses port 80 (HTTP's default port), which is always open and not blocked or filtered by the firewall. In this article, the SQL injection attack and ways for exploiting it were examined, and the methods were classified based on the approach used to exploit them. The work on preventing SQL injection attacks has been reviewed, and a novel strategy to preventing such attacks has been proposed and presented.

SQL INJECTION

SQL injection attacks are a form of injection attack in which the attacker inserts SQL commands into the input parameters to affect how the server executes SQL queries (Dalai & Jena, 2017). Attackers exploit situations where developers combine SQL statements with user-submitted parameters, injecting SQL instructions within those parameters to change the pre-defined SQL query. As a result, the attacker can use the application processing layer to execute arbitrary SQL instructions and queries on the database server using the application processing layer (Prokhorenko et al., 2016c). A successful SQL injection attack can access sensitive database data, change data (insert/alter/update/delete), run administrative operations, and get the content of a specified file on the database server, as well as run operating system level commands (Damele & Guimares, 2009). Below is an example of a SQL injection attack. Assume a web page is dynamically produced by using the user's parameter in the URL itself, such as:

http://www.testdomain.com/Admit/Candidates.asp?Sid=199

The SQL query that corresponds to the application code is run, such as

SELECT Name, Branch, Department FROM Candidate WHERE MatricNumber = 199

An attacker might take advantage of the fact that the application accepts the parameter "Sid" and sends it to the database server without any validation or escaping. As a result, the arguments can be tampered with to generate malicious SQL queries. For example, if the variable "Sid" is set to "199 or 2=2," the following URL is generated:

http://www.testdomain.com/Admit/Candidates.asp?Sid=199 or 2=2

The SQL statement will now be transformed into

SELECT Name, Department, Location FROM Candidate WHERE MatricNumber = 199 or 2=2

This condition is always true, and the user will receive all of the Name, Department, and Location triplets. By adding arbitrary SQL instructions, the attacker can further exploit this vulnerability. An attacker may, for example, make a request for the following URL:

http://www.testdomain.com/Admit/Candidates.asp?Sid=199; DROP TABLE Candidate

The semicolon in the above URL stops the server-side SQL query and adds a new one to be executed. The second query is “*DROP TABLE Candidate*” which deletes the table from the database server. An attacker can utilize the “*UNION SELECT*” query to retrieve data from additional tables in a similar fashion. The *UNION SELECT* command allows the results of two distinct *SELECT* queries to be combined.

Many online applications' default security approach treats SQL queries as trusted commands. As a result, attackers can use this flaw to bypass access restrictions, authorisation, and authentication checks. SQL queries can sometimes be used to obtain server operating system commands through stored procedures. In most cases, the database management server includes stored procedures such as the extended stored procedure. “*xp_cmdshell*” is a Microsoft extended stored procedure that is kept in the master database. This process enables you to use T-SQL code to issue operating system commands straight to the Windows command shell. The output of these commands will be returned to the calling function if it is required. As a result, the attacker in the preceding example can set the value of “Sid” to “*199; EXEC master..xp_cmdshell dir --*”; if run, this will return a list of files in the SQL Server process' current directory. The attacker can load and read arbitrary files from the server using *LOAD FILE('xyz.txt')* in MySQL.

STEPS FOR EXPLOITING VULNERABILITIES

Reconnaissance, enumeration, data extraction, and command execution are some of the steps that may be taken to attack the SQL injection vulnerability. The stages are outlined in full below. In this write up Microsoft SQL Server is being used as the main database backend throughout.

Reconnaissance

It is the first and most crucial step in optimizing an application's potential. It's a technique for fingerprinting the technologies used, which helps the attacker conduct a SQL injection attack more successfully. When database server error messages are sent to the client, they may reveal a lot of information about the database server technology that the web application is utilizing. However, if the web application displays a verbose error message supplied by the database, the query “*SELECT @@version*” can be used to acquire precise information about the back-end database server, such as the specific version and patch level. Security and Communication Networks 3 would show up on the screen

Microsoft OLE DB Provider for SQL Server error '80040e0x'Microsoft][ODBC SQL ServerDriver][SQL Server] Conversion failed when converting the varchar value 'Microsoft SQL Server 2008 -9. 0x.13xx.0x (Intel X86) Nov 15 2008 00:33:37 Copyright (c) 198X-2008 Microsoft-Corporation Express Edition on Windows NT 5.5 (Build 379X: Service Pack 2X)' to data type int. /Candidatesx. aspx, line 213

This demonstrates that the victim's back-end is Microsoft SQL Server 2008. It also contains information about the host operating system and the precise build level. As a result, similar approaches may be used to produce more accurate fingerprints for additional bits of information, such as shown in the following table 1.

Table 1: Reconnaissance: Queries which can be used to exploit detailed information about backend servers

	Query	Description
1	@@version	Ver. For DBMS
2	db name()	Database name
3	@@servername	Server name for MS-SQL installation
4	@@language	language name
5	@@spid	ID of current user's Process

Enumeration

To carry out a successful attack and completely exploit the SQL injection vulnerability, you must first list all of the database's tables and column names. Metadata is information on all of the system and user-defined tables that is stored in a database management system's pre-defined tables. As a result, in order to enumerate the database server's tables/columns, the attacker must first get access to those tables. Table 2 presents the queries to retrieve the database name, table name, and column name.

Table 2: Enumeration queries which can be used to exploit detailed information about Databases, Tables and Columns

	Extract	Query
1	Databases	select name from master..sysdatabases
2	Tables	SELECT name FROM Databasename..sysobjects WHERE xtype='U'
3	Columns	SELECT name FROM Databasename..syscolumns WHERE id = (SELECT id FROM Databasename..sysobjects WHERE name = 'Tablename')

Extraction of data

After determining the column, table, and database names, the following step is data extraction from the tables. The "UNION SELECT" query is used to extract the data. The number of columns in the injected query must match the number of columns in the preexisting SELECT query in the UNION SELECT statement. We may use an ORDER BY statement to get the precise number of columns in an existing query. The query must be run again and again until it runs without errors and the number of columns is revealed by the last successfully completed query. The number of columns may also be determined by progressively increasing the number of columns in the "UNION SELECT" expression until the query executes successfully, as shown below.

<http://www.testdomain.com/Admit/Candidates.asp?Sid=199+union+select+1-->
<http://www.testdomain.com/Admit/Candidates.asp?Sid=199+union+select+1,2-->
<http://www.testdomain.com/Admit/Candidates.asp?Sid=199+union+select+1,2,3-->

The UNION operator combines two SELECT queries into one and displays the result. Consequently, you may use the UNION SELECT query to acquire the data you need from the database server. The command will then be executed in the next stage. This phase comprises exploiting the injection flaw to execute system commands. To perform system commands, the current user must have elevated privileges. To run system commands in MS-SQL, use xp cmdshell, such as exec master.xp cmdshell 'ipconfig'.

TYPES OF SQL INJECTION ATTACKS

As numerous research (Al-Khashab et al., 2011; Buehrer et al., 2005; Liu et al., 2009; Yeole & Meshram, 2011) have shown, there are various forms of SQL injection attacks. These attack types were normally called after the techniques used to exploit the injection vulnerability. Tautology, addition of comments, type mismatch, query piggy bank, union query, stored procedure function and inference techniques are discussed in Table 3 below.

Table 3: Types of SQL Injection Attacks, Sample Codes and Explanations

Attack Type	Sample Code	Brief Explanation
1. Tautology	<i>“Select from admin where user id = ‘ ’ and password = ‘ ’ or ‘a’ Equals ‘a’ “</i>	A tautology is a logical assertion that is TRUE regardless of the interpretation (cite,xxxx). The same principle is utilized in SQL queries in the conditional statement, in the <i>WHERE</i> clause, to make it always TRUE and return all data. To conduct the injection attack, this is frequently placed in the susceptible parameter. Tautology is mostly used to get around the login authentication process. Blind SQL injection vulnerability is also confirmed using tautology.
2. Addition of comments	<i>“SELECT * from admin where userid= ‘xxx’; -- and password = ‘yyy’;”</i>	SQL, like other programming languages, allows you to include a comment line in your code. The code can be commented by adding a double hyphen in MS-SQL or a # in MySQL. The code is not executed because of the comment line. The attackers take advantage of this by inserting a comment in the susceptible parameter, which disables the rest of the code that follows the vulnerable parameter. The following is a simple example of how to use a comment line. The above code can bypass the login authentication by giving only valid user id.
3. Type Mismatch	<i>“http://www.testdomain.com/Admit/Candidates.asp?Sid=system user The error output is like [Microsoft][ODBC SQL Server Driver][SQL Server] error: xxx, Conversion failed when converting the varchar value ‘sa’ to data type integer”</i>	The “Type mismatch in expression” error indicates that Access cannot match an input value to the data type it expects for the value. For example, if you give Access a text string when it is expecting a number, you receive a data type mismatch error. In case of type mismatch in the query, SQL provides a verbose error message, for instance, from the above error message, we can clearly know that the current user is ‘sa’; hence, the attacker takes advantage of this and provides type mismatch queries like giving characters to a numeric type and vice versa and can easily extract a lot of information.
4. Query Piggyback		A query that is stacked or piggybacked query is one that executes a series of SQL queries in a single connection to the database server. When opposed to merely injecting code into the original query, the ability to terminate the old query and attach a whole new one while leveraging the fact that the database server would execute both of them gives the attacker greater freedom and options. The stacked query is supported by the majority of database management systems. For <i>ALTER</i> , <i>DELETE</i> , and other operations, stacked queries

		can be constructed and performed. This can have a significant influence on the back-end database.
5.Union Query	<pre> "http://www.testdomain.com/Admit/UNION SELECT Candidates.asp?Sid=199 FROM LOGIN, USERID, AND PASSWORD;" </pre>	<p>This is a query that joins two or more tables together. The union operator takes the results of two <i>SELECT</i> queries and merges them into a single result. As a consequence, after enumerating the table and column names, the vulnerable parameter may be used to inject the <i>UNION SELECT</i> statement, which will combine the results with the original query and obtain the data. The following is an example of how to use <i>UNION SELECT</i>.</p> <p>The userid and password pair will be combined with the original query and shown to the client in the above request. The query may be tweaked further to loop through all of the rows in the login database.</p>
6.Store d Procedure Functions	<pre> "SELECT password hash FROM logins.sys.sqlhttp://www.testdomain.com/Admit/Candidates.asp?Sid=199+union+select+master.varbinto hexstr(password hash)+ dbo.fn where +name='sa'+from+sys.sql+logins" </pre>	<p>A stored procedure in a database management system is a collection of SQL statements that are concatenated to form a process that is saved in the data dictionary. Stored procedures are available in compiled form, allowing many programs to share them. The usage of stored procedures can help with productivity, data integrity, and data access control. These stored procedures can be used by the attacker to have a significant influence on the SQL injection attack. The stored procedure <i>exec master</i> is an example of how to use it.</p> <p>'<i>ipconfig</i>' in <i>xp cmdshell xp cmdshell</i> is an MSSQL extended stored procedure that allows administrators to perform operating system level commands and obtain the necessary results. SQL injection can also be aided by the usage of system defined functions. The <i>sql logins</i> view in SQL Server 2005 stores hashes. The query may be used to get the system hash.</p> <p>The method <i>fn varbinto hexstr()</i> transforms the password hash saved in varbinary form to hex so that it can be viewed in a browser, and then it is decrypted into plain text using tools like "Cain and Abel."</p>
7.Inference	<pre> "http://www.testdomain.com/Admit/Candidates.asp?Sid=199 and SUBSTRING(user name(),1,1)='c' SUBSTRING(user name(),1,1)='c' SUBSTRING(user name — " </pre>	<p>The act or process of drawing logical conclusions is known as inference (cite, xxxx). We use inference to extract information from time to time; for example, "if we receive this output, then this may be occurring at the back-end." By observing the answer to a given query, inference methods can extract at least one item of data. The key is observation, since when the query is true, the answer will have a different signature than when it is false.</p> <p>The states of False and True are determined by the response on the page after each request is received; that is, if the response includes the phrase "no records exist," the state was False; otherwise, the state was True. Similarly, starting with the letter "a" and going through the alphabet, we can deduce all subsequent characters of the USER name by repeating the technique.</p>

ALTERNATIVE METHODS

Input filters are frequently used in web applications to defend against common threats such as SQL injection. Attackers may employ encoding techniques to get around such filters. Case variation, URL encoding, CHAR function, dynamic query execution, null bytes, layering striped expressions, exploiting truncation, and other techniques are used to achieve the approach. The attacker gets through the defense measures by employing the methods listed above. The following are some examples of how to use alternative approaches.

Several strategies for avoiding SQL injection attacks have been developed. One of the most recent security trends is the focus on the security of smart devices that use the Android operating system. Some recent papers (Azfar et al., 2014, 2015, 2016a, 2016c, 2016b, 2017) demonstrate approaches for maintaining security in an Android context. Security in web applications, on the other hand, cannot be overlooked due to its widespread use. These strategies are presented and described in Table 4: Strategies for Avoiding SQL Injection Attacks (Refer to the table 4)

Table 4: Strategies for Avoiding SQL Injection Attacks

	Strategy	Description	References
1	Static Evaluation.	Some techniques depend solely on static examination of source code. These approaches examine the program and utilize heuristics or information flow analysis to find code that is vulnerable to SQL injection attacks. Before being included into the query, each and every user input is scrutinized. These approaches can yield false positives due to the inaccuracy of the static analysis that is being performed. Furthermore, because the approach depends on declassification criteria to turn untrustworthy data into more reliable data, it may result in false negatives. To identify whether an application may create questions that include tautologies, Wassermann and Su offer an approach that combines static analysis and automated reasoning techniques. The sorts of SQL injection attacks that this method may identify are restricted.	(Gould et al., 2004; Lam et al., n.d.; Livshits & Lam, 2005; Wassermann & Su, 2004; Xie & Aiken, 2006)
2	Runtime Monitoring and Static Analysis	AMNESIA (Analysis and Monitoring for Neutralizing SQL Injection Attack) is an approach that combines static analysis with runtime monitoring. They create legitimate queries in the static part, which the application can generate automatically. In the dynamic section, the dynamically built runtime questions are monitored and confirmed for compatibility with the static part's queries.	(Halfond & Orso, 2005b, 2005a, 2006)

3	Context-Oriented Approach	Prokhorenko's context-oriented approach provides a unique way for protecting web applications against many sorts of attacks. This paper provides a single general solution for many forms of web application injection attacks. The authors have chosen a different approach to the vulnerability's underlying cause. The typical attack features are examined in this paper, and a context-oriented model for web application protection is built as a result. The presence of a backdoor in the code, on the other hand, may be undetected by the model. The method may not be able to work as intended if code obfuscation, code hiding, and other techniques are used. A general and extendable PHP-oriented protection framework is provided by Prokhorenko et al. The suggested framework is mostly dependent on the application developer's knowledge of his or her intentions. It monitors the execution in real time and detects deviations from the planned behavior, assisting in the prevention of potentially harmful activities. This approach is just for detecting attacks in the PHP environment of 6 Security and Communication Networks. If the application is built with a technology other than PHP, this technique will fail to defend against assaults.	(Prokhorenko et al., 2016a, 2016b)
4	Validation of input.	The incorrect separation of code and input data is the source of many injection problems. As a result, different approaches based on input validation have been presented. Controlling the flow of user input through the secure gateway is done using Security Policy Descriptor Language (SPDL) By imposing user input limitations, the defined policy analyzes and modifies each request/response. PowerForms all utilize a similar approach. These signature-based methods may have insufficient input validation processes, resulting in false positives. Because these methods are reliant on humans, determining the data that needs to be filtered and the policy that should be implemented takes a lot of time.	(Brabrand et al., 2000; Kareem et al., 2021; Khalaf et al., 2021; D. J. Scott, 2005; D. Scott & Sharp, 2002)
5	Randomization of Instruction Sets.	Each term and operator in all SQL statements in the programme code is assigned a random token using a technique called SQLrand. The query is double-checked before being submitted to the database to ensure that all operators and keywords include the token. The assaults would be readily identified because the attacker's operators and keywords do not contain that token. This method is cumbersome because it requires randomising both the underlying SQL parser in the database and the SQL statements in the computer code. When the random tag is applied to the entire SQL statement and each phrase, the query becomes arbitrarily long. It's also vulnerable to brute-force attacks if you use this method.	(Boyd & Keromytis, 2004)

6	Anomaly Detection or Learning-Based Methods	To learn all of the required query structure statically or dynamically a variety of learning-based methods has been suggested. The integrity or precision of the learning algorithms determines how successful detection is.	(Asmawi et al., 2008; Halfond & Orso, 2005a; Jia Yew et al., 2014; Lee et al., 2002; Valeur et al., 2005)
---	---	--	---

PERFORMANCE METRICS

The Table 5 describes performance metrics which can be utilized to evaluate the effectiveness of the suggested model were the False Acceptance Rate (FAR), Genuine Acceptance Rate (GAR), False Rejection Rate (FRR), Receiver Operating Characteristics (ROC) curve, and Area Under ROC curve (AUC). For the full description refer to Table 5: Performance Evaluation Metrics for Model Effectiveness.

Table 5: Performance Evaluation Metrics for Model Effectiveness

	Performance Metric	Description	Reference
1	Rate of False Acceptance (FAR).	The frequency of attack vectors that can get past the attack detection mechanism is measured in FAR. This statistic is intended to assess how well the suggested strategy performs in the attack detection mode. When the application server's security system fails to intercept a malicious web request, the query with SQL injection code is transmitted to the database server for execution, resulting in a false acceptance.	(Arora & Kumar, 2021; Chakladar et al., 2021; Chandra et al., 2021; J. Chen et al., 2021; Hammad & Wang, 2019; Tomar & Singh, 2021; Wan et al., 2021)
2	Genuine Acceptance Rate (GAR).	The frequency of acceptance in relation to the legitimate web requests provided for execution is referred to as GAR. These data are intended to assess the proposed approach's performance when utilized in attack verification mode. When a legitimate web request is categorized as a regular (nonattack) pattern, it is said to be genuine.	(Hammad & Wang, 2019)
3	Rate of False Rejection (FRR).	The frequency of rejections in relation to the number of valid web requests that should be forwarded for execution is referred to as the FRR. These data are used to evaluate how well the proposed method performs in the verification mode. When a legitimate web request is misclassified as malicious, a false rejection occurs.	(Arora & Kumar, 2021; Chakladar et al., 2021; D. Chen et al., 2021; J. Chen et al., 2021; Hammad & Wang, 2019; Wan et al., 2021)

4	Operational Characteristics of the Receiver (ROC).	The ROC curve shows the relationship between GAR (Genuine Acceptance Rate) and FAR as the threshold value changes. Linear, logarithmic, and semilogarithmic scales are used to plot the curve.	(Chandra et al., 2021; Hammad & Wang, 2019; Tomar & Singh, 2021; Wan et al., 2021)
5	The Surface of the ROC Curve (AUC).	The Area Under the Curve (AUC) is the percentage of coverage under the ROC curve. The more coverage the system has, the more accurate it is. In an ideal world, GAR = 1 at FRR = 0 for a system with 100 percent accuracy, resulting in AUC = 100 percent.	(Natole, 2020; Yang et al., 2021; Yuan et al., n.d.)
6	Error Rates Are Equal (EER).	The EER is the point on a ROC curve when the FAR and FRR are equal. As a result, a lower EER implies higher performance. Table 1 and Figure 8 show that the suggested technique produces good results. The suggested solution is then compared to current strategies in terms of their ability to fight against different forms of SQL injection attacks. The results demonstrate that the proposed model outperforms its competitors. The results of comparisons with known techniques are summarized in Table 2. It is obvious that the suggested technique is resistant to all forms of SQL injection attacks.	(Chandra et al., 2021; Hammad & Wang, 2019; Tomar & Singh, 2021)

CONCLUSION

SQL injection attacks remain at the top long-term running threat to the web and its resources. Presented is a review of the steps which include reconnaissance, enumeration, and extraction of data. Also discussed are types of injection attacks including tautologies, addition of comments, type mismatch, query piggy backing, union query, inference, and stored procedures. Some alternative procedures for mitigating SQL attacks were also discussed which included static evaluation and static analysis, runtime monitoring, content-oriented approach, validation of input, randomization of instruction sets, anomaly detection and learning based methods. Performance metrics for measuring the effectiveness of SQL injection mitigation techniques were presented last which included, rate of false acceptance (FAR), genuine acceptance rate (GAR), rate of false rejection (FRR), Operational characteristics of the receiver (ROC) surface of ROC curve (AUC) and equal error rates. To check for fraudulent input, the paper suggests successively extracting the intended user input from the dynamic query string.

AUTHOR BIOGRAPHY

Aduragbemi David Ogundijo is student of the postgraduate programme PhD (Information Technology) at Infrastructure University Kuala Lumpur (IUKL) Faculty of Engineering, Science and Technology. He holds a BSc in IT (Software Engineering), MSc in Information Systems. His research interests are mainly in mitigating SQL Injection Attacks Email: aduragbemi.ogundijo@gmail.com.

Atiff Abdalla Mahmoud Arabi is student of the postgraduate programme PhD (Information Technology) at Infrastructure University Kuala Lumpur (IUKL) Faculty of Engineering, Science and Technology. He obtained his BIT and Masters in IT in Networking from IUKL. His research interests

include Zero Trust, Biometrics Authentication, and Prevention of Network-Based Academic Dishonesty. Email: atiff2009@gmail.com

Tadiwa Elisha Nyamasvisva, PhD is a member at the Faculty of Engineering and Science Technology in IUKL. His research interests are in Computer Algorithm Development, Data Analysis, Networking and Network Security, and IT in Education. Email: tadiwa.elisha@iukl.edu.my

REFERENCES

- Al-Ahmad, H., Atan, R., Azim, A., Ghani, A., & Murad, M. A. (2014). SOFTWARE MAINTAINABILITY ASSESSMENT BASED ON COLLABORATIVE CMMI MODEL. *Infrastructure University Kuala Lumpur Research Journal*, 2(1).
- Al-Khashab, E., Al-Anzi, F. S., & Salman, A. A. (2011). PSIAQOP: Preventing SQL Injection Attacks based on query optimization process. Proceedings of the 2nd Kuwait Conference on E-Services and e-Systems, KCESS'11. <https://doi.org/10.1145/2107556.2107566>
- Aniche, M., Bavota, G., Treude, C., Gerosa, M. A., & van Deursen, A. (2018). Code smells for Model-View-Controller architectures. *Empirical Software Engineering*, 23(4), 2121–2157. <https://doi.org/10.1007/s10664-017-9540-2>
- Arora, M., & Kumar, M. (2021). AutoFER: PCA and PSO based automatic facial emotion recognition. *Multimedia Tools and Applications*, 80(2), 3039–3049. <https://doi.org/10.1007/s11042-020-09726-4>
- Asmawi, A., Sidek, Z. M., & Razak, S. A. (2008). System architecture for SQL injection and insider misuse detection system for DBMS. Proceedings - International Symposium on Information Technology 2008, ITSIM, 3, 4–9. <https://doi.org/10.1109/ITSIM.2008.4631942>
- Azfar, A., Choo, K. K. R., & Liu, L. (2014). A study of ten popular Android mobile VoIP applications: Are the communications encrypted? Proceedings of the Annual Hawaii International Conference on System Sciences, 4858–4867. <https://doi.org/10.1109/HICSS.2014.596>
- Azfar, A., Choo, K. K. R., & Liu, L. (2015). Forensic taxonomy of popular Android mHealth apps. 2015 Americas Conference on Information Systems, AMCIS 2015, August, 13–15.
- Azfar, A., Choo, K. K. R., & Liu, L. (2016a). An Android Communication App Forensic Taxonomy. *Journal of Forensic Sciences*, 61(5), 1337–1350. <https://doi.org/10.1111/1556-4029.13164>
- Azfar, A., Choo, K. K. R., & Liu, L. (2016b). An android social app forensics adversary model. Proceedings of the Annual Hawaii International Conference on System Sciences, 2016-March, 5597–5606. <https://doi.org/10.1109/HICSS.2016.693>
- Azfar, A., Choo, K. K. R., & Liu, L. (2016c). Android mobile VoIP apps: a survey and examination of their security and privacy. *Electronic Commerce Research*, 16(1), 73–111. <https://doi.org/10.1007/s10660-015-9208-1>
- Azfar, A., Choo, K. K. R., & Liu, L. (2017). Forensic taxonomy of android productivity apps. *Multimedia Tools and Applications*, 76(3), 3313–3341. <https://doi.org/10.1007/s11042-016-3718-2>
- Brabrand, C., Møller, A., Christensen, R. M., & Schwartzbach, M. I. (2000). PowerForms: Declarative Client-Side Form Field Validation. BRICS Report Series, 7(43), 1–20. <https://doi.org/10.7146/brics.v7i43.20210>
- Buehrer, G., Weide, B. W., & Sivilotti, P. A. G. (2005). Using parse tree validation to prevent SQL injection attacks. SEM 2005 - Proceedings of the 5th International Workshop on Software Engineering and Middleware, September, 106–113. <https://doi.org/10.1145/1108473.1108496>
- Chakladar, D. das, Kumar, P., Roy, P. P., Dogra, D. P., Scheme, E., & Chang, V. (2021). A multimodal-Siamese Neural Network (mSNN) for person verification using signatures and EEG. *Information Fusion*, 71, 17–27. <https://doi.org/10.1016/j.inffus.2021.01.004>

- Chandra, S., Singh, K. K., Kumar, S., Ganesh, K. V. K. S., Sravya, L., & Kumar, B. P. (2021). A novel approach to validate online signature using machine learning based on dynamic features. *Neural Computing and Applications*, 33(19), 12347–12366. <https://doi.org/10.1007/s00521-021-05838-6>
- Chen, D., Yan, Q., Wu, C., & Zhao, J. (2021). SQL Injection Attack Detection and Prevention Techniques Using Deep Learning. *Journal of Physics: Conference Series*, 1757(1). <https://doi.org/10.1088/1742-6596/1757/1/012055>
- Chen, J., Cai, L., Tu, Y., Dong, R., An, D., & Zhang, B. (2021). An Identity Authentication Method Based on Multi-modal Feature Fusion. *Journal of Physics: Conference Series*, 1883(1). <https://doi.org/10.1088/1742-6596/1883/1/012060>
- Dalai, A. K., & Jena, S. K. (2017). Neutralizing SQL injection attack using server side code modification in web applications. *Security and Communication Networks*, 2017. <https://doi.org/10.1155/2017/3825373>
- Gould, C., Su, Z., & Devanbu, P. (2004). JDBC checker: A static analysis tool for SQL/JDBC applications. *Proceedings - International Conference on Software Engineering*, 26(June 2004), 697–698. <https://doi.org/10.1109/icse.2004.1317494>
- Halfond, W. G. J., & Orso, A. (2005a). AMNESIA: Analysis and monitoring for NEutralizing SQL-injection attacks. 20th IEEE/ACM International Conference on Automated Software Engineering, ASE 2005, 174–183. <https://doi.org/10.1145/1101908.1101935>
- Halfond, W. G. J., & Orso, A. (2005b). Combining static analysis and runtime monitoring to counter SQL-injection attacks. 1–7. <https://doi.org/10.1145/1083246.1083250>
- Halfond, W. G. J., & Orso, A. (2006). Preventing SQL injection attacks using AMNESIA. *Proceedings - International Conference on Software Engineering*, 2006, 795–798. <https://doi.org/10.1145/1134285.1134416>
- Hammad, M., & Wang, K. (2019). Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network. *Computers and Security*, 81, 107–122. <https://doi.org/10.1016/j.cose.2018.11.003>
- Jia Yew, T., bin Samsudin, K., Izura Udzir, N., & Jahari bin Hashim, S. (2014). BUFFER OVERFLOW ATTACK MITIGATION VIA TRUSTED PLATFORM MODULE (TPM). *Infrastructure University Kuala Lumpur Research Journal*, 2(1).
- Kareem, F. Q., Ameen, S. Y., Salih, A. A., Ahmed, D. M., Kak, S. F., Yasin, H. M., Ibrahim, I. M., Ahmed, A. M., Rashid, Z. N., & Omar, N. (2021). SQL Injection Attacks Prevention System Technology: Review. *Asian Journal of Research in Computer Science*, 13–32. <https://doi.org/10.9734/ajrcos/2021/v10i330242>
- Khalaf, O. I., Sokiyna, M., Alotaibi, Y., Alsufyani, A., & Alghamdi, S. (2021). Web attack detection using the input validation method: Dpda theory. *Computers, Materials and Continua*, 68(3), 3167–3184. <https://doi.org/10.32604/cmc.2021.016099>
- Lam, M. S., Whaley, J., Livshits, V. B., Martin, M. C., & Carbin, M. (n.d.). Context-Sensitive Program Analysis as Database Queries.
- Lee, S. Y., Low, W. L., & Wong, P. Y. (2002). Learning Fingerprints for a. *Architecture*, 264–279.
- Liu, A., Yuan, Y., Wijesekera, D., & Stavrou, A. (2009). SQLProb: A proxy-based architecture towards preventing SQL injection attacks. *Proceedings of the ACM Symposium on Applied Computing*, 2054–2061. <https://doi.org/10.1145/1529282.1529737>
- Livshits, V. B., & Lam, M. S. (2005). Finding Security Errors in Java Programs with Static Analysis. *Proc. Usenix Security Symposium*, 271–286.
- Natole, M. J. (2020). Fast Optimization Algorithms For AUC.
- Paolone, G., Paesani, R., Marinelli, M., & Felice, P. di. (2021). Empirical Assessment of the Quality of MVC Web Applications Returned by xGenerator. <https://doi.org/10.3390/computers>

- Prokhorenko, V., Choo, K. K. R., & Ashman, H. (2016a). Context-oriented web application protection model. *Applied Mathematics and Computation*, 285, 59–78. <https://doi.org/10.1016/j.amc.2016.03.026>
- Prokhorenko, V., Choo, K. K. R., & Ashman, H. (2016b). Intent-Based Extensible Real-Time PHP Supervision Framework. *IEEE Transactions on Information Forensics and Security*, 11(10), 2215–2226. <https://doi.org/10.1109/TIFS.2016.2569063>
- Scott, D. J. (2005). Abstracting application-level security policy for ubiquitous computing. <http://www.cl.cam.ac.uk/>
- Scott, D., & Sharp, R. (2002). Developing secure web applications. *IEEE Internet Computing*, 6(6), 38–45. <https://doi.org/10.1109/MIC.2002.1067735>
- Tomar, P., & Singh, R. C. (2021). Cascade-based Multimodal Biometric Recognition System with Fingerprint and Face. *Macromolecular Symposia*, 397(1). <https://doi.org/10.1002/masy.202000271>
- Valeur, F., Mutz, D., & Vigna, G. (2005). A learning-based approach to the detection of SQL attacks. *Lecture Notes in Computer Science*, 3548(Detection of Intrusions and Malware, and Vulnerability Assessment: Second International Conference, DIMVA 2005. Proceedings), 123–140. https://doi.org/10.1007/11506881_8
- Wan, J., Chen, Y., & Bai, B. (2021). Joint feature extraction and classification in a unified framework for cost-sensitive face recognition. *Pattern Recognition*, 115. <https://doi.org/10.1016/j.patcog.2021.107927>
- Wassermann, G., & Su, Z. (2004). An analysis framework for security in Web applications. *SAVCBS 2004 Specification and Verification of Component-Based Systems*, 70.
- Xie, Y., & Aiken, A. (2006). Static detection of security vulnerabilities in scripting languages. *15th USENIX Security Symposium*, 179–192.
- Yang, Z., Xu, Q., Bao, S., He, Y., Cao, X., & Huang, Q. (2021). When All We Need is a Piece of the Pie: A Generic Framework for Optimizing Two-way Partial AUC framework Image Processing View project Saliency Detection with Comprehensive Information View project When All We Need is a Piece of the Pie: A Generic Framework for Optimizing Two-way Partial AUC. <https://www.researchgate.net/publication/354047024>
- Yeole, A. S., & Meshram, B. B. (2011). Analysis of different technique for detection of SQL injection. *International Conference and Workshop on Emerging Trends in Technology 2011, ICWET 2011 - Conference Proceedings, Icwet*, 963–966. <https://doi.org/10.1145/1980022.1980229>
- Yuan, Z., Guo, Z., Xu, Y., Ying, Y., & Yang, T. (n.d.). Federated Deep AUC Maximization for Heterogeneous Data with a Constant Communication Complexity. Retrieved January 12, 2022, from www.libauc.org

TECHNOLOGY ACCEPTANCE IN TOURISM SECTOR: A SYSTEMATIC REVIEW

Sulaiman Al Jahwari¹, Mohd. Dan Bin Jantan¹, and Supriya Pulparambil²

¹*Infrastructure University Kuala Lumpur, MALAYSIA*

²*Oman College of Management and Technology, OMAN*

ABSTRACT

The emergence of innovative technologies has a significant impact on promoting tourism. Determining how to use these technologies for tourism marketing is very vital for tourism promotion. Technology acceptance by tourists is the initial step towards technology adoption. Taking this into account, this research provides a systematic review of the technology acceptance studies specific to the tourism sector. The objective of this research is to review the trend and acceptance of various information and communication technologies (ICT) in the tourism sector. This research conducted a systematic review of tourism-specific technology acceptance articles published between 2010 and 2021 in online databases. From an analysis of 35 primary manuscripts published in the last 10 years, the study has concluded that the technology acceptance model (TAM) has been mostly applied to measure the online experiences of technology adoption rather than the onsite experience. Despite the positives of the identified TAM-based research models, the study also reports research gaps specific to the context of technology adoption for tourism. The study has theoretical and practical implications. From a theoretical perspective, this study summarizes the recent technological developments in the tourism sector and reports the gaps in technology acceptance studies. Practitioners can use the study results to identify the scope of emerging technologies to improve and market tourism services. The review has selected only three digital libraries which may exclude relevant articles in the context of TAM in tourism.

Keywords:

Tourism, Technology Acceptance, TAM, Technology Adoption, Behavioural Intention

INTRODUCTION

The tourism sector is recognized as one of the important sectors for the economic diversification plan of different nations (Tanfeedh, 2017). Tourism marketing can be looked at from the lenses of demand and supply (Middleton et al., 2009; Middleton & Clarke, 2012). The product supply at destinations includes the activities, attractions, events, and facilities. Normally, the tour operator promotes tourism destinations by putting site attractions in the website, brochures, messages etc. The lack of unique tourism activities and insufficient marketing is a major challenge faced by the tourism sector in many countries. To strengthen tourism marketing and attract more visitors, information technologies are widely used. UN world tourism organization has identified three main functions of tourism marketing: (i) establishment of customer contacts, (ii) development includes the innovations for new sales opportunities, and (iii) control includes the activities to analyse the results of promotion (Lomova et al., 2016). The role of technologies in destination marketing has been a research interest for the last two decades (Li, Robinson, & Oriade, 2017). Digital marketing technologies are reconfiguring the tourism industry (Andreea, 2014; Huang et al., 2016; Levitskaya & Yanioglo, 2019) by offering instant access to all kinds of information to customers. However, recent research has shown that there is a wide gap between the overly made 'claims' and the actual 'realities' about the potential of emerging technologies for marketing (Moorhouse et al., 2018). This is mainly because of the challenges faced by destination marketing organizations in creating a virtual world, handling the bigger data volume over social media, and lack of control over individual user-generated content (Li et al., 2017).

The fourth industrial revolution and convergence of innovative technologies, such as the internet of things, virtual reality (VR), augmented reality (AR), geo-spatial data and broadband, artificial intelligence, and big data are promoting a dramatic shift towards more data and machine-driven marketing initiatives in tourism sector (Sarkady & Egger, 2021; Yoo et al., 2017). The new technology developments in the travel and tourism sectors also promise better customer experiences and satisfaction. The technologies like VR and AR also open a new dimension for tourism, i.e. virtual tourism; a travel substitution during the COVID pandemic to experience different tourism sites (Sarkady & Egger, 2021). Considering the wide adoption of various emerging technologies to promote tourism, a primary question that arises is how the acceptance of these technologies are evaluated.

Most technology adoption studies in the tourism sector use TAM as the basic theory to evaluate technology acceptance among users. TAM was initially proposed in 1986 (Davis et al., 1989) for predicting user acceptance of ICT based on the theory of reasoned action (Lai, 2017). The TAM considers two aspects of technology usage: perceived usefulness and perceived ease of use. A large number of research papers have been published on the usage of TAM to evaluate the tourists' motivation and perception (Li & Chen, 2019). Tourism sector is adopting different types of technologies at the sites to provide better tourism experience and heightening the level of tourist satisfaction and enjoyment (Buhalis, 2019). TAM has been explored to understand the factors of human behaviour that determine the technology acceptance or rejection. Nevertheless, there is a gap that exists in current knowledge on the applicability of TAM to evaluate the acceptance of technologies that create empowered tourism experiences. It is useful to understand the applications of the TAM in this aspect; however, a systematic analysis of TAM in the tourism sector is still lacking in academic literature. A systematic literature review is selected as a research method to understand and analyse the applications of the TAM in the tourism sector. The main objective of this review is to understand how TAM-based research models are applied in the context of technology adoption in the tourism sector.

The contributions of this research can be looked at from three different aspects: (i) provides an overview of technology trends adopted in the travel and tourism sector, (ii) summarizes the research models based on TAM for tourism, and (iii) summarizes the research gaps in evaluating technology acceptance in the tourism sector. The review helped to understand the recent technical developments in the tourism sector and the prevalent areas of TAM applications. The review observed that travel information systems and mobile software are widely used applications before or during the travel. The ease of use and usefulness of these applications are the major determinants of their acceptance. On the other hand, most of the studies applied TAM from an individual perspective for assessing tourist's behaviour intentions to use such technologies. Besides, the review presented a summary of the variables studied in the context of technology acceptance and helped to identify other theories combined with TAM to explore different dimensions of technology acceptance. Among the selected studies, 40% of them focused on the visit intention and the impact of online tourism marketing tools. Finally, the review concluded that the existing TAM-based research models need to explore parameters that could connect with the user emotions while utilising emerging technologies such as digital immersive technologies, robotics, or recommender systems.

The review results open further scope for improvements in assessing technology adoption in the tourism sector. In conclusion, this study presents a future research agenda to be worked on. The rest of the paper is organized as follows. Section 2 presents a review of TAM models. Section 3 details the research design. Section 4 discusses the results and presents answers to the research questions through a framework. Section 5 discusses our future research agenda and section 6 concludes the review.

LITERATURE REVIEW

TAM was initially proposed in 1986 (Davis et al., 1989) for predicting user acceptance of ICTs. The TAM is based on two aspects of technology usage: perceived usefulness (PU) and perceived ease of use (PEU). The perceived usefulness is the user's belief that the system will increase his job performance. Perceived ease of use is the degree to which the user believes that system usage is free of effort (Davis et al., 1989). The TAM model is very simple because it focusses only on two constructs for assessing the behavioural intention to use the technology. The external variables are the different factors that influence the PU and PEU. The PEU also influences the PU; hence PU can be a variable of type both dependent and independent. Both PU and PEU influence the attitudes to use technology. The user's attitude to use the technology determines the intention to use the technology and thereby the actual use of technology occurs. In 1996, the TAM model was modified by analysing the impact of perceived usefulness and ease of use on behaviour intention (Davis & Venkatesh, 1996) and excluded the attitude variable from the TAM model because of the direct impact of perceived usefulness and perceived ease of use on behavioural intention to use the technology.

In 2000, an extended version of TAM was published as TAM 2 (Venkatesh & Davis, 2000). The user acceptance of ICT is analysed by considering both social influence and cognitive instrumental processes. The subjective norm, image, and voluntariness indicate people's perception of system usage. The job relevance, output quality, and result demonstrability represent the magnitudes of job tasks performed by the system. In basic TAM model, the authors found that subjective norm has no impact on perceived ease of use, perceived usefulness, and intention to use the system; however, TAM 2 claims that the subjective norm, image, and voluntariness are also the determinants of using or rejecting a system. TAM 2 extends the basic TAM with additional variables. TAM 2 proved that subjective norm has a positive impact on the intention to use the system when it is mandatory; hence voluntariness act as a moderator between intention to use the system and subjective norm. Similarly, the TAM 2 proves that subjective norm has a positive influence on perceived usefulness and image. The positive effect of the image, job relevance, output quality, and result demonstrability on perceived usefulness is also confirmed. The study also confirms that the impact of these determinants will change as the experiences in system usage increase. It is worth noting that TAM 2 focused on perceived usefulness and further research on the perceived ease of use to refine TAM 2 has been done and as a result, TAM 3 (Venkatesh & Bala, 2008) is developed.

TAM 3 is different from its previous versions by analysing the parameters that influence the managerial decisions on implementing technologies. TAM 3 is an integrated model of TAM 2 and the determining factors of perceived ease of use. The identified determinants are computer self-efficacy, perception of external control, computer anxiety, computer playfulness, perceived enjoyment, and objective usability (Venkatesh & Bala, 2008). The model states that these determinants of perceived ease of use do not influence perceived usefulness. TAM 3 confirms the moderating effects of experience in three relations: (i) the impact of perceived ease of use on perceived usefulness, (ii) the impact of computer anxiety on perceived ease of use, and (iii) the effect of perceived ease of use on behavioural intention to use the system. All these models are developed to evaluate the intention to use a system or technology based on two primary constructs, i.e. perceived ease of use and perceived usefulness.

Most of the technology adoption studies use the traditional TAM as the basic theory (Davis et al., 1989) to evaluate its acceptance among users. Many studies have been published on the acceptance of TAM to study tourists' motivation or perception (Li & Chen, 2019). Considering the wide adoption of various emerging technologies to promote tourism, TAM is a theoretical foundation to establish the acceptance or rejection of a particular technology.

RESEARCH METHOD

A considerable amount of literature has been published about technology adoption in the tourism domain. A systematic review is conducted to classify existing literature that applied TAM in the tourism sector. The research method has three steps: planning, conducting, and mapping. In the planning phase, the research questions and the review protocol were defined. The review protocol includes the data sources, search strategies used, period coverage for primary study selection, and exclusion criteria for paper screening. In the conducting phase, the defined search strings were searched in the repositories based on the review protocol. The initial search results were analysed to identify the relevant studies based on inclusion, exclusion, and quality criteria. The data needed to answer the research questions were extracted from relevant studies and the results are synthesized. In the mapping phase, the selected studies are classified to extract knowledge.

This study will provide answers to two main research questions: (i) What are the contexts for using TAM in the tourism sector? What are the behavioural dimensions of technology adoption in the tourism domain and the factors that determine it? The search was performed in electronic databases such as Google Scholar (<https://scholar.google.com/>), Springer (<http://www.springerlink.com>), and ScienceDirect (<http://www.sciencedirect.com>). All the mentioned databases have an advanced search option to refine the search results. The study applied this option to limit the search to specific years and metadata such as title, abstract, and keywords. The advanced search option for sources is slightly different from each other. The keywords were used to identify all the primary studies under the scope of research. The identified keywords are ‘Tourism’, ‘technology acceptance model’, and ‘TAM’. The search strategy has considered the AND/OR combinations of keywords (‘TAM or ‘technology acceptance model’) AND (‘tourism’). The study considered only the publications between 2010 and 2020.

The study found 204 publications, whose title or abstract had the keywords defined in the search strategy. Using advanced search strategies, duplicates and non-English papers were excluded thus resulting in 117 papers. Study selection is a multistage process. In the first stage, duplicates from three electronic databases were removed, and articles were reviewed against exclusion and inclusion criteria. Studies published in other languages are excluded. A study with substantial information on technology adoption in tourism has been only selected for further review. As a result, 57 relevant articles are qualified for the second stage review. In the second stage, the abstracts and keywords are reviewed to exclude the documents with insufficient information. As a result, 35 studies were selected for further analysis as listed in Appendix. The selected papers are carefully read through to mitigate the misinterpretations of the title and abstract. The extracted results are reported through different graphs.

RESULTS

In this section, the results of the review are presented as answers to the two research questions. The technology adoption in the tourism domain (Hamdan & Yusof, 2014) is dynamically growing to support both tourists and tourism providers. First, the context of TAM application is discussed, followed by various behavioural intentions in the context of technology adoption for the tourism sector.

Applications of TAM

The first question of this study was meant to classify the TAM studies based on their technologies evaluated. TAM is used to validate the acceptance of information technology (Davis et al., 1989) in many sectors. It has been observed that TAM is widely applied in both the travel and tourism industry

to understand tourists' behaviour intention on adopting various technologies. Thus, the selected studies are first analysed to understand the context of TAM usage and the type of technologies implemented. The technological developments in tourism have a crucial role in deciding where to travel in terms of selecting destinations based on social networking feedback or conducting a virtual tour using software applications before travel. In the same direction, ICT is used to collect information about tourism sites as well as for travel guidance. The selected studies can be broadly classified into eight groups based on their technology services, as shown in Table 1.

Table 1: Technology Services

Technology service	Remark	Reference
Digitized information and services	Information about tourism sites and their services to guide tourists.	(Lin et al., 2014; Wang et al., 2015)
Online visual experience	Visuals of the tourism spot through websites and applications to explore the destination before travel	(Chiao et al., 2018; Huang et al., 2013; tom Dieck & Jung, 2018; Xia et al., 2018)
Onsite visual experience	Visual exhibits at the tourism sites to share more knowledge and entertain tourists	(Hammady & Strathearn, 2020; Sagnier et al., 2020)
Online travel planning services	Services for travel booking and other amenities in advance	(Herrero & San Martín, 2012; Liu et al., 2016; Sahli & Legohérel, 2015; Wang & Jeong, 2018)
Online tourism marketing services	Tourism marketing through social media (e.g. YouTube) and social networking (e.g. Twitter)	(Di Pietro & Pantano, 2013; Gani, 2017; Lee et al., 2013)
Location-based personalized services	Map services and other personalized services based on geographical location	(Chung et al., 2017; Palos-Sanchez et al., 2017)
Games	Online and onsite games for entertainment	(Yoo et al., 2017)
Network connectivity	Internet and other network services like GPS	(Masri et al., 2017)

Most of the technologies are to support tourists either before travel (e.g., travel information systems) or during travel (e.g., navigator systems). The providers are also adopting specific technologies to market tourism (e.g., visual experience technologies). Travel information systems and various types of mobile software (Kaur et al., 2016) are used to get tourism site information and tourist feedback. The gamified applications at tourism sites are mainly to enhance tourists' loyalty and memorable experiences. The tourism sector has also adopted virtual reality and augmented reality applications to market destinations by creating virtual tour experiences. Major tourism sites are providing Wi-Fi and other network connectivity services; location-based services are provided by using the ability of mobile phones to detect geographical locations. Social networking sites are also used as destination marketing tools for tourism services and products.

The technology experience and the type of application differ. Mobile software can be used to know more about the tourism sites; hence it provides digitized information to the tourists. Similarly, another mobile software application can be used to access location-based services such as route maps. In this way, based on their application type they are classified into different groups as shown in Figure 1. Figure 1 presents the technologies evaluated using TAM in the tourism sector and their distribution.

Among the selected studies, mobile software is mostly used as a guidance tool during travel (Chen & Tsai, 2019; Im & Hancer, 2014; Lin et al., 2014) and also to get the visual experience of the tourist spot before travel (Huang et al., 2013; tom Dieck & Jung, 2018; Xia et al., 2018). Another wide scope of ICT adoption is in the area of travel service planning (Cheng & Cho, 2011; Herrero & San Martín, 2012). This includes travel booking (Wang & Jeong, 2018), tourist spot information, recommendations, and other services such as service coupons and offers (Mendes et al., 2016). The new trends of technology adoption revolve around immersive technologies such as VR, AR, and mixed realities (Jung et al., 2020). The VR/AR/mixed reality applications are widely used to provide online visual experience for travellers (Li & Chen, 2019; tom Dieck & Jung, 2018).

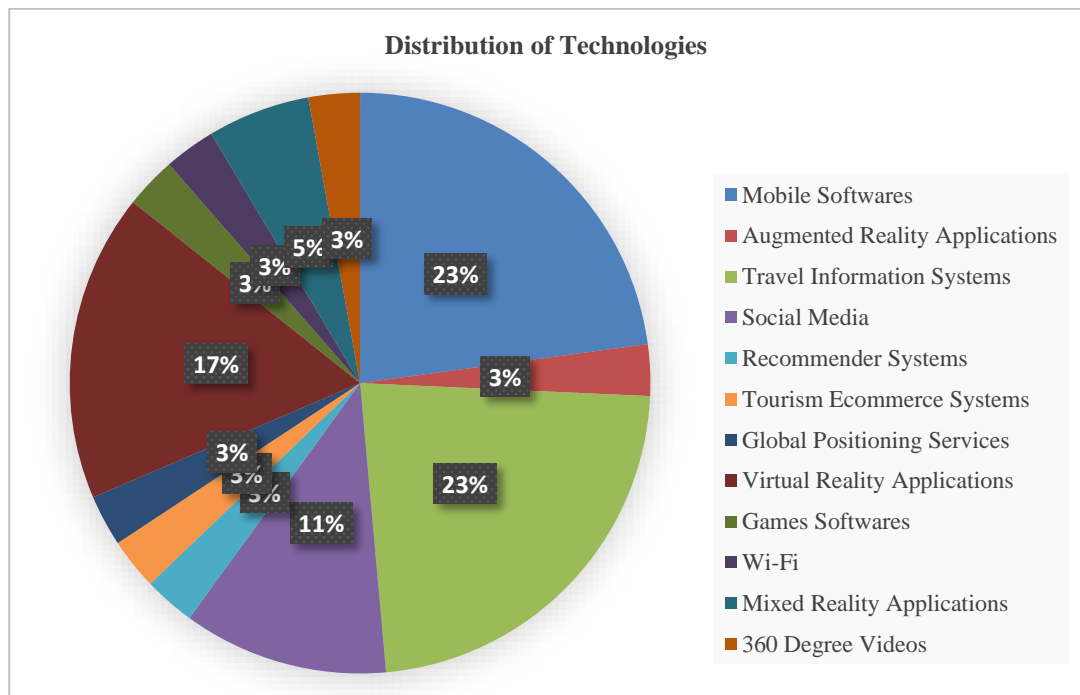


Figure 1: Distribution of Technologies in the Context of TAM

Behavioural Intention in TAM

The second question of this study aims to extract different behavioural intentions and the determinants of technology acceptance. TAM has been applied to understand the technology adoption in different contexts such as providing digitized information of the sites, leisure and utility-based mobile applications, map services, etc. The initial TAM has been modified by analysing the impact of perceived usefulness and ease of use on behaviour intention of users (Davis & Venkatesh, 1996). In 2000, an extended version of TAM is published as TAM 2 (Venkatesh & Davis, 2000). The user acceptance of ICT is analysed by considering both social influence (Mohammed et al., 2020) and cognitive instrumental processes. Similarly, in 2008 TAM 3 was published (Venkatesh & Bala, 2008); it is different from its previous versions by analysing the parameters that influence the managerial decisions on implementing technologies. However, most of the selected studies were focused only on two variables perceived usefulness and perceived ease of use in determining the behavioural intention of tourists.

Any theoretical research model or framework is supported by different kinds of variables. The variables can be external, independent variables (IVs), mediators, or dependent variables (DVs). Most of the selected studies have proposed new research models based on TAM. The variables and their relation differ in each study. Considering that, this research reviewed the IVs, mediators, and DVs of each study. The summary of the DV distribution among selected studies is given in Figure 2.

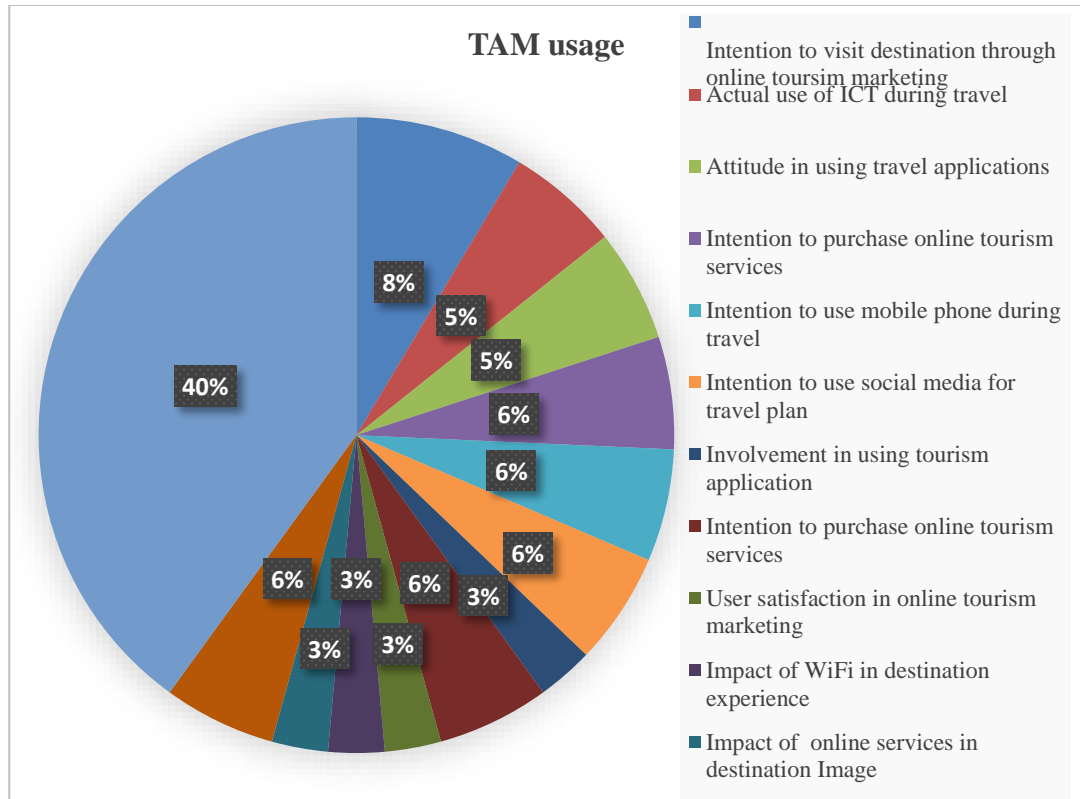


Figure 2: Distribution of Dependent Variables in the Context of TAM

Almost all the studies have considered ‘perceived usefulness’ and ‘perceived ease of use’. A few studies (Cheng & Cho, 2011; Di Pietro & Pantano, 2013; Im & Hancer, 2014; Masri et al., 2017; O’ Regan & Chang, 2015; Wang & Jeong, 2018; Wang et al., 2015) included additional IVs with TAM. Another interesting variable is ‘perceived enjoyment’ (PE), which is considered as an IV in five models and as the mediator in another five models. Similar to the basic TAM, nine models have adopted ‘attitude’ as a mediator. The remaining variables are unique and depend on the context. Most of the models have ‘behaviour intention’ as the DV. However, based on the technology context it differs e.g. ‘Behaviour intention to use mobile technologies’. Most of the models used basic TAM theory and defined additional variables. However, a few studies have integrated TAM and other theories. It is important to note that four TAM-based theoretical models merged flow theory (Liu et al., 2016; Sahli & Legohere, 2015; Wang et al., 2015; Yoo et al., 2017) with TAM and two studies focused on the theory of planned behaviour (Cheng & Cho, 2011; Sahli & Legohere, 2015) and innovation diffusion theory (Cheng & Cho, 2011; Wang & Jeong, 2018).

DISCUSSION

The research questions aimed at providing a comprehensive overview of the TAM and its applications in the tourism sector. The analysis of the studied models mainly helped to explore what kind of technologies are implemented in the tourism domain and the factors that determine various behavioural intentions of visitors through the lenses of TAM. With regards to technology adoption, the research models have already been explored for technology acceptance, behavioural intention to use the technologies and its impact on tourism marketing by promoting the destination image. There is also a necessity to understand different parameters that could connect to user emotions with the influence of emerging technologies, especially digital immersive technologies.

According to the travel and tourism competitiveness report for 2019, the future of the current tourism industry is technology-driven (Calderwood & Soshkin, 2019). This report shows that the first 25 ranks of the travel and tourism competitiveness index are bagged by developed countries. However, there are few developing countries like Brazil, India, and Thailand that are in the first 50 only because of their rich cultural and natural resources. Hence, another interesting research area within the context of technology adoption is the type of technologies required to promote cultural and heritage tourism. As already discussed, most of the technology adoption studies are providing online services for tourists. This clearly shows the gap that exists in implementing technologies to promote tourism by providing technology services at the tourism sites. The onsite experience is expected to increase destination attachment and thereby promote revisits. This study shows that there are limited studies on onsite technology implementation and their acceptance to provide a better experience for tourists. The growing interest in digital immersive technologies (to provide more visual appeal) in the tourism domain has attracted much attention from researchers (Beck et al., 2019; Bogicevic et al., 2019; Jung et al., 2015; Moorhouse et al., 2018; Oliveira & Correa, 2017; Yung & Khoo-Lattimore, 2017). Their potential in various contexts is explored; however, limited studies have explored their role in promoting cultural and heritage tourism (Buonincontri & Marasco, 2017; Trunfio et al., 2018; Yung & Khoo-Lattimore, 2017).

The analysis also concluded that value and experience attributes are explored very minimally in the context of technology acceptance in tourism. Considering 'perceived value' as a multidimensional construct, it has different views such as emotional value, social value, utilitarian, and hedonic value aspects (Lee et al., 2011). However, the factors associated with value perspectives are not much explored by the existing models. Among the selected TAM studies, only one study considered perceived value as a mediator (Koo et al., 2017); however, they analysed perceived value from a cost and benefit perspective. They neither considered the social or emotional attributes of perceived value. Another two studies considered emotional attachment (O' Regan & Chang, 2015), and emotional involvement (Huang et al., 2013) in adopting emerging technologies for tourism. Hence, the review opens a research question on the parameters to be explored to understand the multi-dimensionality of value aspects within the context of technology adoption. This leads to the further question: "What are the value parameters to be considered while assessing the acceptance of emerging technologies in the context of tourism?". The influence of these value parameters in promoting tourism needs to be investigated. Despite the positives of the identified models, the following knowledge is still lacking and that has to be further looked into by researchers.

- *Onsite experience: More than 70% of the existing technology acceptance studies in the tourism domain are mainly for providing digitized information, online travel planning, and social media applications. The technologies to enhance the onsite experience of tourists are less explored.*
- *User experience aspects: Most of the models have not considered the emotional aspects of user experiences. It is important to note that a few studies have considered enjoyment aspects (Huang et al., 2013, 2016); however, the entertainment and education aspects are less explored in the context of technology adoption.*

- *A value-based acceptance model: To the best of our knowledge, none of these models except (Koo et al., 2017) have considered value factors. This is very critical in the context of technology adoption as most of the ICT adoption falls under the service category.*

The above conclusions show that future research is essential to address the identified gaps. At a fundamental level, further investigation is required on (i) adopting technologies at tourism sites to enhance site experience, (ii) best practices for digital technologies to promote cultural and heritage tourism, and (iii) a TAM-based research model with value-based parameters to evaluate the acceptance of technologies by tourists.

CONCLUSION

This paper presents the results of a review on the applicability of TAM to measure the acceptance of various technology adoptions in the tourism domain. The review has selected 35 primary studies that have applied TAM in the last decade for the tourism sector. This review establishes that TAM has been widely used to evaluate the behaviour intentions of tourists to use mobile-based software for travel guidance and visual experiences to understand tourism spots. Similarly, tour operators and tourism providers are adopting emerging technologies to market their tourism initiatives. It has been observed that most of the technology investments by tourism providers are service-based and mostly provide online experiences for tourists. The new technological developments bring many opportunities to enhance tourists' experience through different platforms such as the internet of things, mobility services, travel booking, and payment services, voice recognition and translation services, robotic devices, and virtual and augmented reality applications (Bu, 2018). The determinants of their acceptance vary according to context.

The research has both theoretical and practical impacts. The study reports further scope for improvements in assessing technology adoption in the tourism sector. Practitioners can use the results to identify gaps in emerging technology adoption to improve and market tourism services. The study reports possible improvements for TAM to evaluate tourists' onsite experiences of technologies. However, this study has considered a period of the last ten years and the search has been limited to only three electronic databases. The study results reveal that TAM has been applied from an individual perspective and organization require TAM-based research models to assess the technology acceptance, and this has to be looked into. Future research on technology acceptance in the tourism domain should consider value and experience-based constructs.

AUTHOR BIOGRAPHY

Sulaiman Al Jahwari (MSc from Manchester Metropolitan University, UK) is a Ph.D. student (Business Administration and Marketing) in Infrastructure Kuala Lumpur University, Malaysia. His research interest is the best practices and approaches for Oman tourism marketing based on emerging technologies. *Email: sjahwari72@gmail.com*

Mohd. Dan Bin Jantan, PhD. Graduated from Northern Illinois University, USA and is an Associate Professor in Business, Information, and Human Sciences Faculty of Infrastructure University Kuala Lumpur, Malaysia. He has more than fifteen years of teaching experience. He has also worked as a project leader and researcher in several funded research projects. *Email: djantan@iukl.edu.my*

Supriya Pulparambil (Ph.D. from Sultan Qaboos University, Oman) is an Assistant Professor in Computer Science and Management Information Systems Department, Oman College of Management and Technology, Oman. Her research interest includes information systems, software engineering, software quality assurance, service-oriented architecture, digital transformation, and sustainable smart cities. Email: supriya.pulparambil@omancollege.edu.om

REFERENCES

- Andreea, M. (2014). *the Emerging Technological Trends in the Tourism Industry*. 73–76.
- Beck, J., Rainoldi, M., & Egger, R. (2019). Virtual reality in tourism: a state-of-the-art review. *Tourism Review*, 74(3), 586–612. <https://doi.org/10.1108/TR-03-2017-0049>
- Bogicevic, V., Seo, S., Kandampully, J. A., Liu, S. Q., & Rudd, N. A. (2019). Virtual reality presence as a preamble of tourism experience: The role of mental imagery. *Tourism Management*, 74, 55–64. <https://doi.org/10.1016/j.tourman.2019.02.009>
- Bu, N. (2018). The 22nd Session of the UNWTO General Assembly – Special Session on Smart Tourism. *Anatolia*, 29(1), 143–145. <https://doi.org/10.1080/13032917.2017.1393720>
- Buhalis, D. (2019). Technology in tourism-from information communication technologies to eTourism and smart tourism towards ambient intelligence tourism: a perspective article. *Tourism Review*, 75(1), 267–272. <https://doi.org/10.1108/TR-06-2019-0258>
- Buonincontri, P., & Marasco, A. (2017). Enhancing Cultural Heritage Experiences with Smart Technologies : An Integrated Experiential Framework. *European Journal of Tourism Research*, 17, 83–102.
- Calderwood, L., & Soshkin, M. (2019). The Travel & Tourism Competitiveness Report 2019. In *Tourism*. World Economic Forum. http://www3.weforum.org/docs/WEF_TTCR_2019.pdf
- Chang, P. (2017). The Importance Performance Analysis of Taiwan Tourism Mobile Marketing. *Journal of Tourism Management Research*, 4(1), 12–16. <https://doi.org/10.18488/journal.31/2017.4.1/31.1.12.16>
- Chen, C. C., & Tsai, J. L. (2019). Determinants of behavioral intention to use the Personalized Location-based Mobile Tourism Application: An empirical study by integrating TAM with ISSM. *Future Generation Computer Systems*, 96, 628–638. <https://doi.org/10.1016/j.future.2017.02.028>
- Cheng, S., & Cho, V. (2011). An integrated model of employees' behavioral intention toward innovative information and communication technologies in travel agencies. *Journal of Hospitality and Tourism Research*, 35(4), 488–510. <https://doi.org/10.1177/1096348010384598>
- Chiao, H. M., Chen, Y. L., & Huang, W. H. (2018). Examining the usability of an online virtual tour-guiding platform for cultural tourism education. *Journal of Hospitality, Leisure, Sport and Tourism Education*, 23, 29–38. <https://doi.org/10.1016/j.jhlste.2018.05.002>
- Chung, N., Tyan, I., & Han, H. (2017). Enhancing the smart tourism experience through geotag. *Information System Frontiers*, 19(4), 731–742. <https://doi.org/10.1007/s10796-016-9710-6>
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, 35(8), 982–1003.
- Davis, F. D., & Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. *International Journal of Human-Computer Studies*, 45(1), 19–45.
- Di Pietro, L., & Pantano, E. (2013). Social network influences on young tourists: An exploratory analysis of determinants of the purchasing intention. *Journal of Direct, Data and Digital Marketing Practice*, 15(1), 4–19. <https://doi.org/10.1057/dddmp.2013.33>
- Gani, A. A. (2017). Social media information and hotel selection : Integration of TAM and IAM

- models. *Celebrating Hospitality and Tourism Research*, 9(2), 113–124.
- Ghanem, M. M., Mansour, S. O., & Adel, H. (2017). The impact of national culture on the adoption of e-tourism in Egyptian tourism companies. *Tourism*, 65(2), 234–246.
- Hamdan, N., & Yusof, A. (2014). Determining demographic profiles and tourists' motives for visiting Langkawi Island. *Infrastructure University Kuala Lumpur Research Journal*, 2(1), 1–43.
- Hammady, R., & Strathearn, C. (2020). Ambient Information Visualisation and Visitors' Technology Acceptance of Mixed Reality in Museums. *ACM Journal on Computing and Cultural Heritage*, 13(2).
- Herrero, Á., & San Martín, H. (2012). Developing and testing a global model to explain the adoption of websites by users in rural tourism accommodations. *International Journal of Hospitality Management*, 31(4), 1178–1186. <https://doi.org/10.1016/j.ijhm.2012.02.005>
- Huang, Y. C., Backman, K. F., Backman, S. J., & Chang, L. L. (2016). Exploring the implications of virtual reality technology in tourism marketing: An integrated research framework. *International Journal of Tourism Research*, 18(2), 116–128.
- Huang, Y. C., Backman, S. J., Backman, K. F., & Moore, D. W. (2013). Exploring user acceptance of 3D virtual worlds in travel and tourism marketing. *Tourism Management*, 36, 490–501. <https://doi.org/10.1016/j.tourman.2012.09.009>
- Im, J. Y., & Hancer, M. (2014). Shaping travelers' attitude toward travel mobile applications. *Journal of Hospitality and Tourism Technology*, 5(2), 177–193. <https://doi.org/10.1108/JHTT-11-2013-0036>
- Jung, K., Nguyen, V. T., Piscarac, D., & Yoo, S. C. (2020). Meet the virtual jeju dol harubang—The mixed VR/Ar application for cultural immersion in Korea's main heritage. *ISPRS International Journal of Geo-Information*, 9(6). <https://doi.org/10.3390/ijgi9060367>
- Jung, T., Chung, N., & Leue, M. C. (2015). The determinants of recommendations to use augmented reality technologies: The case of a Korean theme park. *Tourism Management*, 49, 75–86. <https://doi.org/10.1016/j.tourman.2015.02.013>
- Kaur, K., Salome, S., & Muthiah, S. (2016). Harnessing the power of mobile technology: A look at Malaysian mobile commerce landscape. *Infrastructure University Kuala Lumpur Research Journal*, 4(1), 41–46. <https://iukl.edu.my/rmc/wp-content/uploads/sites/4/2018/04/5.-Harnessing-the-Power-of-Mobile-Technology-A-Look-at-Malaysian-Mobile-Commerce-Landscape.pdf>
- Koo, C., Chung, N., & Ham, J. (2017). Assessing the user resistance to recommender systems in exhibition. *Sustainability*, 9(11), 20–41. <https://doi.org/10.3390/su9112041>
- Kucukusta, D., Law, R., Besbes, A., & Legohérel, P. (2015). Re-examining perceived usefulness and ease of use in online booking the case of Hong Kong online users. *International Journal of Contemporary Hospitality Management*, 27(2), 185–198. <https://doi.org/10.1108/IJCHM-09-2013-0413>
- Lai, P. (2017). the Literature Review of Technology Adoption Models and Theories for the Novelty Technology. *Journal of Information Systems and Technology Management*, 14(1), 21–38. <https://doi.org/10.4301/s1807-17752017000100002>
- Lee, B. C., Cho, J., & Hwang, D. (2013). An integration of social capital and tourism technology adoption—A case of convention and visitors bureaus. *Tourism and Hospitality Research*, 13(3), 149–165. <https://doi.org/10.1177/1467358414522055>
- Lee, J. S., Lee, C. K., & Choi, Y. (2011). Examining the role of emotional and functional values in festival evaluation. *Journal of Travel Research*, 50(6), 685–696. <https://doi.org/10.1177/0047287510385465>
- Levitskaya, A., & Yanioglo, N. (2019). Digital marketing technologies as an effective tool for promotion of tourism in the republic of Moldova. *Marketing and Digital Technologies*, 2(3), 77–84. <https://doi.org/10.15276/mdt.2.3.2018.5>
- Li, S., Robinson, P., & Oriade, A. (2017). Destination marketing: The use of technology since the

- millennium. *Journal of Destination Marketing and Management*, 6(2), 95–102. <https://doi.org/10.1016/j.jdmm.2017.04.008>
- Li, T., & Chen, Y. (2019). Will virtual reality be a double-edged sword? Exploring the moderation effects of the expected enjoyment of a destination on travel intention. *Journal of Destination Marketing and Management*, 12, 15–26. <https://doi.org/10.1016/j.jdmm.2019.02.003>
- Lin, K. C., Chang, L. S., Tseng, C. M., Lin, H. H., Chen, Y. F., & Chao, C. L. (2014). A smartphone APP for health and tourism promotion. *Mathematical Problems in Engineering*, 2014. <https://doi.org/10.1155/2014/583179>
- Liu, Y., Pu, B., Guan, Z., & Yang, Q. (2016). Online customer experience and its relationship to repurchase intention: An empirical case of online travel agencies in China. *Asia Pacific Journal of Tourism Research*, 21(10), 1085–1099. <https://doi.org/10.1080/10941665.2015.1094495>
- Lomova, L. A., Shiryaev, D. V., Kobersy, I. S., Borisova, A. A., & Shkurkin, D. V. (2016). Marketing techniques in management of enterprises engaged in tourism. *International Review of Management and Marketing*, 6(6), 15–20.
- Mang, C. F., Piper, L. A., & Brown, N. R. (2016). The incidence of smartphone usage among tourists. *International Journal of Tourism Research*, 18(6), 591–601.
- Masri, F., Anuar, I., & Yulia, A. (2017). Influence of Wi-Fi service quality towards tourists' satisfaction and dissemination of tourism experience. *Journal of Tourism, Hospitality & Culinary Arts*, 9(2), 383–398. <https://fhtm.uitm.edu.my/v2/images/jthca/Vol9Issue2/4-01.pdf>
- Mendes, L., Jorge, V. A., Júnior, S., & others. (2016). Perception of using group buying sites to acquire tourism services coupons. *Revista Brasileira de Pesquisa Em Turismo*, 10(3), 574–593.
- Middleton, V. T. C., & Clarke, J. R. (2012). *Marketing in travel and tourism*. Routledge.
- Middleton, V. T. C., Fyall, A., Morgan, M., & Ranchhod, A. (2009). Marketing in Travel and Tourism. In *Butterworth-Heinemann* (4th ed.). Elsevier Ltd. https://doi.org/10.1007/978-3-211-93971-0_29
- Mohammed, M. T. S., Ibrahim, F., & Yunus, N. (2020). Conceptual Framework for the Influence of Social Media Usage and Social Media Multitasking on the Academic Performance of the Undergraduate Students. *Infrastructure University Kuala Lumpur Research Journal*, 8 (2), 47–53.
- Moorhouse, N., Jung, T., & tom Dieck, M. C. (2018). The Marketing of Urban Tourism Destinations Through Virtual Reality: Tourism Marketers' Perspectives. *8th Advances in Hospitality and Tourism Marketing And Management (AHTMM) Conference*, 45.
- O' Regan, M., & Chang, H. (2015). Smartphone Adoption amongst Chinese Youth during Leisure-based Tourism: Challenges and Opportunities. *Journal of China Tourism Research*, 11(3), 238–254. <https://doi.org/10.1080/19388160.2015.1077181>
- Oliveira, R. K. de, & Correa, C. (2017). Virtual reality as a tourism marketing strategy. *TURyDES: Revista Turismo y Desarrollo Local*, 10(23). <http://www.eumed.net/rev/turydes/23/virtual-reality.html>
- Palos-Sanchez, P. R., Hernandez-Mogollon, J. M., & Campon-Cerro, A. M. (2017). The behavioral response to Location Based Services: An examination of the influence of social and environmental benefits, and privacy. *Sustainability*, 9(11). <https://doi.org/10.3390/su9111988>
- Rahimizhian, S., Ozturen, A., & Ilkan, M. (2020). Emerging realm of 360-degree technology to promote tourism destination. *Technology in Society*, 63(December 2019), 101411. <https://doi.org/10.1016/j.techsoc.2020.101411>
- Sagnier, C., Loup-Escande, E., Lourdeaux, D., Thouvenin, I., & Valléry, G. (2020). User Acceptance of Virtual Reality: An Extended Technology Acceptance Model. *International Journal of Human-Computer Interaction*, 36(11), 993–1007. <https://doi.org/10.1080/10447318.2019.1708612>
- Sahli, A. B., & Legohérel, P. (2015). The tourism Web acceptance model: A study of intention to book tourism products online. *Journal of Vacation Marketing*, 22(2), 179–194.

- <https://doi.org/10.1177/1356766715607589>
- Sarkady, D., & Egger, R. (2021). Virtual Reality as a Travel Substitution Tool During COVID-19. *Information and Communication Technologies in Tourism 2021*, 1, 452–463. <https://doi.org/10.1007/978-3-030-65785-7>
- Shao, J., Bai, H., Shu, S., & Joppe, M. (2020). Planners' Perception of Using Virtual Reality Technology in Tourism Planning. *E-Review of Tourism Research (ERTR)*, 17(5), 685–695. <http://ertr.tamu.edu>
- Tan, G. W. H., Lee, V. H., Hew, J. J., Ooi, K. B., & Wong, L. W. (2018). The interactive mobile social media advertising: An imminent approach to advertise tourism products and services? *Telematics and Informatics*, 35(8), 2270–2288. <https://doi.org/10.1016/j.tele.2018.09.005>
- Tanfeedh. (2017). *Tanfeedh Handbook*. https://scp.gov.om/PDF/TANFEEDH_HAND_BOOK_2017English.pdf
- Tom Dieck, M. C., & Jung, T. (2018). A theoretical model of mobile augmented reality acceptance in urban heritage tourism. *Current Issues in Tourism*, 21(2), 154–174. <https://doi.org/10.1080/13683500.2015.1070801>
- Trunfio, M., Magnelli, A., Della Lucia, M., Verreschi, G., & Campana, S. (2018). Augmented And Virtual Reality in Cultural Heritage: Enhancing the Visitor Experience and Satisfaction at the Area Pacis Museum In Rome, Italy. In *8th Advances In Hospitality And Tourism Marketing and management (AHTMM) Conference*. <http://www.ahtmm.com/>
- Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, 39(2), 273–315.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186–204.
- Vishwakarma, P., Mukherjee, S., & Datta, B. (2020). Antecedents of Adoption of Virtual Reality in Experiencing Destination: A Study on the Indian Consumers. *Tourism Recreation Research*, 45(1), 42–56. <https://doi.org/10.1080/02508281.2019.1638565>
- Wang, C., & Jeong, M. (2018). What makes you choose Airbnb again? An examination of users' perceptions toward the website and their stay. *International Journal of Hospitality Management*, 74(3), 162–170. <https://doi.org/10.1016/j.ijhm.2018.04.006>
- Wang, J., Wang, M., & Wu, J. (2015). Empirical study on flow experience in china tourism E-commerce market. *Journal of Industrial Engineering and Management*, 8(2), 349–364. <https://doi.org/10.3926/jiem.1393>
- Xia, M., Zhang, Y., & Zhang, C. (2018). A TAM-based approach to explore the effect of online experience on destination image: A smartphone user's perspective. *Journal of Destination Marketing and Management*, 8, 259–270. <https://doi.org/10.1016/j.jdmm.2017.05.002>
- Yoo, C., Kwon, S., Na, H., & Chang, B. (2017). Factors affecting the adoption of gamified smart tourism applications: An integrative approach. *Sustainability*, 9(12), 1–21. <https://doi.org/10.3390/su9122162>
- Yung, R., & Khoo-Lattimore, C. (2017). New realities: a systematic literature review on virtual reality and augmented reality in tourism research. *Current Issues in Tourism*, 3500, 1–26. <https://doi.org/10.1080/13683500.2017.1417359>

APPENDIX

Table 2: Selected Studies

Reference	DV	IV
(Lin et al., 2014)	Acceptance of tourism promotion mobile app	Computer self-efficacy
(Xia et al., 2018)	Acceptance of destination marketing mobile app	PU, PEU
(tom Dieck & Jung, 2018)	Acceptance of augmented reality	PU, PEU
(Cheng & Cho, 2011)	Acceptance of ICT adoption by travel agency employees	PU, PEU, Trialability, Observability, Compatibility, Subjective Norm, Perceived Behavioural Control
(B. C. Lee et al., 2013)	Acceptance of destination marketing through social network	PU, PEU
(Koo et al., 2017)	Acceptance of recommender systems	Self-efficacy, Technical Support, Switching Cost, Relative Advantage
(Chen & Tsai, 2019)	Acceptance of personalized location-based mobile app	Information Quality, System Quality, Perceived convenience
(Herrero & San Martín, 2012)	Acceptance of websites to make reservations	Interactivity, Navigability, Information
(J. Wang et al., 2015)	Acceptance of e-commerce	PU, PEU, PE, Perceived trust
(Chung et al., 2017)	Acceptance of geotagging	Traveller's readiness
(Chiao et al., 2018)	Acceptance of 3D virtual technologies	PU, PEU, perception of autonomy, perception of competence, perception of relatedness
(Huang et al., 2013)	Acceptance 3D virtual technologies	PEU, PU
(Yoo et al., 2017)	Acceptance of gamified smart tourism applications	Flow, Distributive Justice, Network effect, Information quality, Privacy concerns
(Masri et al., 2017)	Acceptance of tourism experiences	Service quality, PU, PEU
(Liu et al., 2016)	Acceptance of Online purchase	Interactive speed, Skill Challenge, Perceived control, Telepresence, PU, PEU
(Mendes et al., 2016)	Acceptance of buying online tourism services coupons from group buying websites	PU, PEU

(Kucukusta et al., 2015)	Acceptance of online bookings	PU, PEU
(Im & Hancer, 2014)	Acceptance of travel applications	PEU, self-identity, PE, PU
(O' Regan & Chang, 2015)	Acceptance of using mobile phones during leisure tourism	PEU, PU, Social influence, Emotional attachment
(Gani, 2017)	Acceptance of the role of social networking in travel decision making	Trust
(Di Pietro & Pantano, 2013)	Behaviour intention to purchase online tourism services	PEU, PU, PE, EWOM communication
(Palos-Sanchez et al., 2017)	Behaviour intention to use location-based services	Privacy, Social and Environmental Benefits
(Ghanem et al., 2017)	Acceptance of actual use of e-commerce for tourism	Uncertainty, Avoidance, Long term orientation
(Chang, 2017)	User satisfaction	PEU, PU, PE
(Mang et al., 2016)	Actual use of mobile phones	UTAUT factors
(Tan et al., 2018)	Acceptance of social media advertising through the mobile app	Mobile self-efficacy, Interactivity, Technology self-efficacy,
(Sahli & Legoharel, 2015)	Intention to book online	PU, PEU, Compatibility, PE, Trust, Perceived benefits, Perceived behavioural control, Subjective norms
(C. Wang & Jeong, 2018)	Acceptance Airbnb websites	PEU, PU, Trust, Amenities, Host guest relationship
(T. Li & Chen, 2019)	Acceptance of virtual reality	PEU, PU
(Rahimizhian et al., 2020)	Acceptance of 360 degree videos	PEU, PU, PE, Immersion, Autonomy
(Shao et al., 2020)	Acceptance of Virtual reality	PEU, PU, Cost, PE, Immersion
(Vishwakarma et al., 2020)	Acceptance of Virtual reality	PEU, PU, PE, Immersion
(Hammady & Strathearn, 2020)	Acceptance of mixed reality	Personal innovativeness
(Sagnier et al., 2020)	Acceptance of virtual reality	Pragmatic quality, hedonic quality, personal innovativeness
(K. Jung et al., 2020)	Acceptance of virtual and augmented reality	Perceived visual design, perceived task-technology

A COMPREHENSIVE SWOT ANALYSIS FOR ZERO TRUST NETWORK SECURITY MODEL

Tadiwa Elisha Nyamasvisva and Atiff Abdalla Mahmoud Arabi
Infrastructure University Kuala Lumpur, MALAYSIA

ABSTRACT

The Zero Trust approach is a cybersecurity preventive measure based on the notion that nothing should be trusted within or near, or outside your network unless their identities are validated. Identities are regularly verified using authentication and authorization mechanisms in this framework. Security does not end once a user enters the network; identities are continually confirmed as they travel across the network. Instead of relying on network perimeters, Zero Trust's approach to security focuses on your identity infrastructure. Systems and networks can no longer rely on a user's affiliation with an organization or the password they supply. Users' traits and activity patterns must be examined by systems and networks to determine who is attempting to access resources, how they might get access, and what they might do with that access. This is a case of Zero Trust. Zero Trust has pros and limitations when compared to other security systems. It is also seen as the final answer to decentralized usage of resources over the internet. This paper's prescription focuses on Zero Trust's strengths, shortcomings, possibilities, and threats.

Keywords:

Virtual Private Networks (VPNs), Multi-Factor Authentication (MFA), Bring Your Own Device (BYOD), Network segmentation, Software Defined Perimeter (SDN)

INTRODUCTION

Security in networks is an evolving challenge that needs to be scrutinized (Andrade, Ortiz-Garces, & Cazares, 2020). Some approaches to network security have worked for extended periods of time with minor alterations to the entire framework of security (Uctu, Alkan, Dogru, & Dörterler, 2019). Significant changes are always required when there are major shakeups at the technology forefront. The introduction of new modern technologies brings about new challenges and always opens once patched loopholes for exploitation (D'Silva & Ambawade, 2021). In traditional network security (Sreeja, Saleem, & Sravya, 2020), security was about protecting the boundaries of the environment; with time more ubiquitous methods started to be introduced.

The recent cybersecurity breaches have had a massive impact. Traditional security measures are ineffective in the face of billions of compromised identities and sensitive data. According to recent data breaches, three out of every five businesses anticipate being hacked. Finding and containing a malicious actor takes an average of 74 days, and privileged credentials are used in 80 percent of breaches. Furthermore, within a 24-hour period, 67 percent of firms penetrated were unable to submit a report indicating who has access to essential systems and accounts (Alkhalil, Hewage, Nawaf, & Khan, 2021). What this demonstrates is that the perimeter as we know it is no longer functional, and the once-defensible perimeter has become the new network attack route (Alkhalil et al., 2021).

Internal and external attacks exploiting current access and compromising the perimeter continue to progress the attack lifecycle (Andrade et al., 2020). Once inside, bad actors can use elevated access to conduct reconnaissance and move laterally through the network, disrupting operations and stealing data (Sreeja et al., 2020).

The infrastructure of a typical business has become increasingly sophisticated. Several internal networks, remote offices with their own local infrastructure, remote and/or mobile personnel, and cloud services may all be run by a single company. Because there is no one readily identifiable border for the company, old perimeter-based network security approaches have been outperformed.

Boundary-based network security has also been proved to be insufficient because once attackers break the perimeter, they have unrestricted access to the whole of the network (Rose, Borchert, Mitchell, & Connelly, 2020).

As a result of this complicated operation, a new cybersecurity paradigm is known as "zero trust" has been developed (ZT). The primary focus of a ZT strategy is data and service security, but it may and should be broadened to encompass all corporate assets and subjects. The term "zero trust" refers to a security reaction to corporate network developments such as remote users, bring your own device (BYOD), and cloud-based assets that are not within an enterprise-owned network perimeter. This is a common practice in industry and education as the focus centered more on cloud and cloud-related activities (Abu-Asba, Azman, Mustaffa, & Ali, n.d.; Hasan, Ibrahim, Mustapha, Islam, & Al Younus, 2018).

BACKGROUND

From the network perimeters, a typical model for network security oversees access to an organization's networks and related assets, resources, and apps (Sreeja et al., 2020). This is known as the castle and trench paradigm, and it involves the deployment of security protocols such as firewalls, Virtual Private Networks (VPNs), access controls, email security, online security, and Security Information and Event Management (SIEM), including self-defined algorithms for tracking users (Sibghatullah H M, Elisha Tadiwa, Atiff Abdalla Mahmoud, Abudhahir, & Fares Anwar Salem, 2021) to name a few. Table 1 below outlines some of the classic network security techniques over time.

Table 1: Timeline of Security Approaches

Period	Security Approaches
Before 2000	Firewall with MDS and Bastion Host
	VLAN infrastructure
	QoS
2000 to 2010	The extension of VM
	VL and virtual network environments,
	Multiple DMZ with VPN concentrators
	Multi-factor for remote access.
	IDS
	IPS
	802.1x
Comprehensive QoS and PoS across both LAN and WAN	
2010 till 2020	Network Segmentation
	Next generation firewalls
	Identity and Access management

However, as more businesses migrate from on-site to hybrid settings and cloud environments, and as several employees work remotely and with their own devices, it is becoming more challenging to safeguard network perimeters and keep track of who goes laterally within the network (Sreeja et al., 2020). As a result, businesses are taking a broader approach to network security.

ZERO TRUST AS A COMPLETE SOLUTION

VPNs and SDNs complement each other when it comes to network security (Van Der Pol, Gijsen, Zuraniewski, Romão, & Kaat, 2016). These approaches are ok to some extent, but they are not comprehensive enough to completely secure network-based resources. There are several issues related to traditional networks, including but not limited to;

- i. Lack of principle of least privilege (PoLP).
- ii. Noncompliance to multi-factor authentication (MFA)
- iii. No use of micro-segmentation.
- iv. Lack of audit to the network.

The growing complexity of dynamic workloads moving across the data center and multi-cloud environments, remote users, and endpoints, combined with a flood of new vulnerabilities and risks from hackers and targeted threats such as ransomware and malware outbreaks, have exposed the inadequacy of traditional security models (Greenwood, 2021). Zero Trust addresses the four shortcomings as part of its offering (Simpson & Foltz, 2021). Adopting Zero Trust architecture is more important than ever since most businesses operate in a multi-cloud environment with distributed and remote workforces. An identity-centric approach to your Zero Trust model should be at the centre of your organization's security architecture. (Atiff, David, & Elisha, 2021).

The Zero Trust Security idea adopts a new access model in which all users are seen as untrustworthy (Chen et al., 2020; Xiaojian, Liandong, Jie, Xiangqun, & Qi, 2021). It represents a paradigm change away from traditional perimeter-based access and toward a user-centric strategy (Redondi, Chirico, Borsani, Cesana, & Tagliasacchi, 2013; Vanickis, Jacob, Dehghanzadeh, & Lee, 2018). Zero Trust is an all-encompassing security approach for people, apps, data, and networks that combines strong authentication principles, multi-factor authentication, step-up authentication, and the use of contextual access limitations and interrogation (Mehraj & Banday, 2020).

“Never trust, always verify.” This Zero Trust philosophy-turned-strategy fundamentally changes the way security is approached since trust is a vulnerability that can be exploited (Wylde, 2021). Cloud applications and security are treated equally to on-premises systems and apps under the Zero Trust approach (Rodigari, O’Shea, McCarthy, McCarry, & McSweeney, 2021). For improved identification of risks and breaches, the model supports the use of sophisticated analytics, artificial intelligence, and machine learning. To implement Zero Trust successfully, these three stages are proposed for a holistic and highly effective security strategy for Zero Trust. The three stages are the discovery stage, the definition stage, and the enforcement stage. Table 2 below describes these three stages.

Table 2: ZT Implementation Guidelines

Stage	Process	Description
1	Discovery	<ul style="list-style-type: none"> - Determine how users, devices, and apps are connected. - Real-time mapping across endpoints and applications - Mapping of sensitive data across users, devices, networks, workloads, and applications - Enabling a single source of truth
2	Definition	<ul style="list-style-type: none"> - Micro-segmentation controls - Automated policy creation. - Compensation of control when it cannot be patched. - Visualize and test policies
3	Enforcement	<ul style="list-style-type: none"> - Enable a default-deny policy - Secure data in transit

		<ul style="list-style-type: none"> - Continuous monitoring - Dynamic Zero Trust policies - Seamless integration with third-party IT tools
--	--	--

The discovery process is used to determine what should be permitted to communicate based on the principle of least privilege. The discovery approach also encourages cooperation by including business and IT stakeholders in the creation of Zero Trust micro perimeters and security regulations. Understanding what is communicating and what should not be communicating is crucial in the discovery process as a vital initial step. By defining and automating the appropriate amount of Zero Trust segmentation rules across endpoints, the described process assures risk reduction and reduces deployment complexity. The second phase is likewise in charge of enforcement, ensuring that when offering security at birth in cloud-native apps, no applications are broken. Using an allow list, enforcement enables a decoupled default-deny policy to implement effective Zero Trust rules wherever your endpoints and workloads are located. Without needing any adjustments or upgrades to the existing network, data in transit is safeguarded.

ZT STRENGTHS

Many of the pillars upon which IT and security are based may be strengthened by incorporating Zero Trust into the core of an organization's infrastructure. Zero Trust can help companies enhance their security posture and restrict their attack surface by introducing some fundamental barriers to entry and enabling access on an as-needed basis, whether it's in fortifying identity and access controls or segmenting data. Table 3 below describes the strengths of Zero trust.

Table 3: The strengths of Zero Trust

No	Strength	Explanation
1	Less vulnerability	<ul style="list-style-type: none"> - The Zero Trust paradigm improves the company's security, particularly against in-network lateral attacks that may appear under a different security model.
2	Strong policies for user identification and access.	<ul style="list-style-type: none"> - Zero Trust necessitates tight user control within the network, resulting in more secure accounts. - Using multi-factor authentication, which goes beyond passwords and includes biometrics, as an effective technique to keep accounts secure. - Categorization of users for the purpose of allowing them access to data and accounts as needed for their job duties.
3	Smart segmentation of data.	<ul style="list-style-type: none"> - Dividing a company's network into compartments, protecting critical intellectual property from illegal users - Lowering the attack surface by keeping susceptible systems well-protected - Threats should not be allowed to migrate laterally across the network. - Reducing the effects of insider threats, particularly those that may endanger employees physically.
4	Increased data protection.	<ul style="list-style-type: none"> - Keeping data secure in both storage and transit. - Backups that are automated are encrypted and hashed, and the message transmission is encrypted and hashed.

		<ul style="list-style-type: none"> - Restricting data access - By segmenting the assault surface, we may reduce the attack surface. - Edge encryption, scrambled data, automatic backups, and leaky bucket security
5	Good security orchestration	<ul style="list-style-type: none"> - Make sure that all of your security features function together efficiently and effectively, with no gaps left unfilled and the integrated elements complementing one another rather than showing inconsistencies between them. - Zero Trust guarantees that security solutions integrate smoothly and cover all potential attack routes. - Finding the optimal settings to enhance productivity while minimizing disputes.

In a Zero Trust paradigm, there would be no one large pool of data that all users could access. (Ahmed, Nahar, Urmi, & Taher, 2020). Data may be segmented by kind, sensitivity, and purpose for a more secure arrangement. This protects essential or sensitive data while reducing potential attack surfaces. Without adequate data and resource segregation, robust access controls won't make sense with Zero Trust. The necessity of security orchestration runs across all of these pillars. Organizations employing Zero Trust would need to guarantee that security solutions function effectively together and cover all potential attack vectors even if they didn't have a security management system (Mehraj & Bandy, 2020). Overlap isn't an issue in and of itself, but finding the optimal settings to enhance efficiency while minimizing conflicts may be difficult.

ZT WEAKNESSES

With all of these added security benefits, the Zero Trust approach complicates security policies. Here are some of the extra obstacles that such a thorough plan entails. (See table 4):

Table 4: The Weaknesses of Zero Trust

No	Weakness	Explanation
1	Time and effort to set up.	<ul style="list-style-type: none"> - Challenging in reorganizing policies within an established network. - Maintaining functionality during the shift. - Better to design a new network from scratch and then shift over. - Incompatible Legacy networks with the Zero Trust architecture require starting from scratch.
2	Increased management of varied users.	<ul style="list-style-type: none"> - It may be challenging to reorganize policies inside the existing network while they continue to function during the transition. - Preferable to design a new network from scratch and then shift over. - If legacy systems are incompatible with the Zero Trust architecture, the process must be restarted.
3	More devices to manage.	<ul style="list-style-type: none"> - Current work environments comprise not only diverse sorts of workers but also varied types of equipment.

		- Different devices with unique attributes and connection methods must be monitored and protected always.
4	More complicated application management.	- A more comprehensive range of varying applications. - Cloud-based apps are frequently used across various platforms. They may be disclosed to third parties. - App use should be planned, monitored, and designed in accordance with a Zero Trust attitude.
5	More careful data security.	- Data is being housed in several locations, which means there are more places to defend. - Data configuration must be done responsibly and in accordance with the highest security requirements.

ZT OPPORTUNITIES

The Zero Trust approach does not explicitly call for achieving complete effectiveness. Zero Trust emphasizes that businesses must start with the user's identification. A solid identity governance and management plan must be in place. As the name implies, Zero Trust offers a surplus of possibilities. See table 5 below.

Table 5: The Opportunities of Zero Trust

No	Opportunity	Explanation
1	Principle of least privilege (PoLP)	The Zero Trust principle is based on the Principle of Least Privilege (PoLP) (DelBene, Medin, & Murray, 2019; Mehraj & Banday, 2020). The concept of least privilege, often known as least privilege access, is a security protocol that assumes that everyone is a potential danger and that; as a result, they should only be provided the rights necessary to accomplish their job function. The notion of least privilege may be extended to programmes, apps, systems, and gadgets in addition to human users (Christ, 2021; Gómez, Alonso-Zárate, Verikoukis, Pérez-Neira, & Alonso, 2007). By restricting user access from within the network, least privilege access helps to protect and secure privileged credentials, data, and assets. As a result, if an attacker gains access to your IT environment, PoLP minimizes their chances of acquiring access to a privileged account, lowering the risk of a data breach.
2	Multi-factor authentication (MFA)	Authentication should be at the heart of every cybersecurity strategy, especially in the case of Zero Trust (Stafford, 2020). There are several authentication techniques available, but multi-factor authentication provides an extra degree of protection by requiring a user to give various pieces of proof (factors) in order to validate their identity and obtain access to a network or multi-cloud environment (Uttecht, 2020). Methods of multi-factor authentication for verification include: <ol style="list-style-type: none"> i. "Something you know: username, password, or pin number." ii. "Something you have: mobile device or app." iii. "Something you are: biometrics such as a fingerprint, face, or voice recognition software"

3	Micro-segmentation.	Micro-segmentation divides a data centre or cloud environment into different segments, limiting user access to specific regions based on their organizational position (Mujib & Sari, 2020). As a result, the user and their workload are protected and isolated to a single network segment until they have the authorization to travel elsewhere. It provides insight into all network activity, allowing administrators to create exact segmentation based on what they see and prevent any risks from spreading laterally across the network. (Sheikh, Pawar, & Lawrence, 2021).
4	Network Audit.	Your Zero Trust solution must be implemented for all users and systems in your IT ecosystem in order to be effective (Li, Zhang, Lei, & Song, 2022). Begin by auditing the identities, access limitations, and access policies on your network. Understanding where your data and applications live, as well as access policies and access controls such as who has access and how they use that access, are vital stages of considering as you begin to develop the security and access protocols for your network.
5	Assured Security	Adoption of an identity and access management system capable of validating these users' identities before granting them access to your network and apps, provisioning access based on user roles, and using policy management to automate, regulate, and monitor how their access is used within the network. A firm Zero Trust policy ensures the safety of all users, apps, and data.

Opportunities from Zero Trust largely present themselves within the versatile identity strategies, which vary according to the application domain and are never similar in many instances. These should include but are not limited to:

- Identity governance controls for roles, entitlements, appropriateness, and SOD policies, as well as risk
- Lifecycle automation for all identities, including workers, contractors, business partners, and machines
- Strong/multi-factor authentication and credential management
- Privileged account and entitlement management
- Centralized application access and self-service fulfillment
- Certification, auditing, and reporting of access

ZT THREATS

There will always be some dangers when a novel solution to a complex problem evolves and appears over time. It takes more than a shift in thinking to implement a Zero Trust security strategy in a business. It will necessitate a thorough understanding of the company's departments' functions, present software, access levels, and devices, as well as what each of those requirements will look like in the future. This is the most severe danger. Because the existing network must stay operational during the transition time, constructing a Zero Trust network from the bottom up is often easier than reconfiguring an existing network into Zero Trust. In all circumstances, IT and security teams should develop a strategy that includes the ideal ultimate infrastructure as well as a step-by-step plan for getting there.

CONCLUSION

Zero Trust as a concept is not a specific product or solution. It is a paradigm shift in the way we think about security. People are the new security perimeter, according to Zero Trust. The new firewall is identity, and it should be at the heart of every Zero Trust plan. Analytics provide an extensive context for access control choices, policy enforcement, and abnormal activity identification. An identification strategy makes access simple and safe while also ensuring that it is the correct access at the right time. To reduce the danger of entitlement creep, orphaned accounts, and separation of duties and appropriateness policies, the strategy should define and regulate access permissions. When properly deployed, the solution will reveal who has access to what and when. Who should have access to the information? What are they going to do with it now that they have it?

Access control is critical in the Zero Trust strategy. During the authentication and authorization process, identity context is reviewed to ensure that a user is who they say they are, that they are using the correct device and that they are accessing the network from an authorized location. This is to control premeditated unauthorized dishonest activities (Elisha Tadiwa Nyamasvisva, Atiff Abdalla Mahmoud Arabi, Abudhahir Buhari, Fares Anwar Hasan, 2020; Nyamasvisva, Atiff Abdalla Mahmoud Arabi, Buhari, & Wong, 2020). Identity identifies and grants the access they should have while also eliminating any access that is inappropriate, unneeded, or no longer required. An identification approach should comprise high-value assets (HVA), sensitive and critical data, structured applications, unstructured data, hosts, and networks. Cloud and on-premises apps should be considered similar and regulated centrally by the Identity platform. Advanced analytics, artificial intelligence, and machine learning benefit all identification data and occurrences. Continuous review and oversight of assignments, rules, and risk, as well as identifying orphaned, potentially toxic, overexposed, or unauthorized access, and revealing behavioral and historical events that may indicate hazardous behavior or malicious intent, are all strengths of Zero Trust. Table 6 summarizes the benefits, drawbacks, opportunities, and dangers of adopting Zero Trust as the final solution to existing security concerns.

Table 6: SWOT analysis of the Zero Trust Model

<p>Strengths</p> <ul style="list-style-type: none"> • Less vulnerability • Strong user identity policies • Smart data segmentation • Enhanced data protection • Great security instrumentation 	<p>Weaknesses</p> <ul style="list-style-type: none"> • Increased setup time • Increased management of varied users • Additional devices to deal with • Additional complex application administration • More careful data security
<p>Opportunities</p> <ul style="list-style-type: none"> • Principle of least privilege (PoLP) • Multi-factor authentication (MFA) • Micro-segmentation • Network Audit • Assured Security 	<p>Threats</p> <ul style="list-style-type: none"> • Implementation • Different environmental challenges • Imported risks from third-party software • Evolving technologies that need constant monitoring

AUTHOR BIOGRAPHY

Tadiwa Elisha Nyamasvisva, PhD is a member at the Faculty of Engineering and Science Technology in IUKL. His research interests are in Computer Algorithm Development, Data Analysis, Networking and Network Security, and IT in Education. Email: tadiwa.elisha@iukl.edu.my

Atiff Abdalla Mahmoud Arabi is student of the postgraduate programme PhD (Information Technology) at Infrastructure University Kuala Lumpur (IUKL) Faculty of Engineering, Science and Technology. He obtained his BIT and Masters in IT in Networking from IUKL. His research interests include Zero Trust, Biometrics Authentication, and Prevention of Network-Based Academic Dishonesty. Email: atiff2009@gmail.com

REFERENCES

- Abu-Asba, A., Azman, H., Mustaffa, R., & Ali, F. (n.d.). TEACHING STYLES OF YEMENI SCIENCE TEACHERS. *RESEARCH JOURNAL (IUKLRJ)*, 53.
- Ahmed, I., Nahar, T., Urmi, S. S., & Taher, K. A. (2020). Protection of sensitive data in zero trust model. *Proceedings of the International Conference on Computing Advancements*, 1–5.
- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, 563060.
- Andrade, R. O., Ortiz-Garces, I., & Cazares, M. (2020). Cybersecurity attacks on smart home during Covid-19 pandemic. *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020*, (October 2020), 398–404. <https://doi.org/10.1109/WorldS450073.2020.9210363>
- Atiff, A., David, A., & Elisha, T. (2021). *A Zero-Trust Model-Based Framework For Managing Of Academic Dishonesty In Institutes Of Higher Learning*. 12(6), 5381–5389.
- Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., ... Zhai, Y. (2020). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, 8(13), 10248–10263.
- Christ, B. (2021). Maturing operational security with an automation-first approach to IAM. *Cyber Security: A Peer-Reviewed Journal*, 5(2), 126–134.
- D’Silva, D., & Ambawade, D. D. (2021). Building A Zero Trust Architecture Using Kubernetes. *2021 6th International Conference for Convergence in Technology (I2CT)*, 1–8. <https://doi.org/10.1109/I2CT51068.2021.9418203>
- DelBene, K., Medin, M., & Murray, R. (2019). The Road to Zero Trust (Security). *DIB Zero Trust White Paper*, 9.
- Elisha Tadiwa Nyamasvisva, Atiff Abdalla Mahmoud Arabi, Abudhahir Buhari, Fares Anwar Hasan, J. R. (2020). Prevalence of Premeditated Academic Dishonesty at University Level. A Case Study. *JOURNAL OF CRITICAL REVIEWS*, 7(15), 4494–4501. <https://doi.org/10.31838/jcr.07.15.598>
- Gómez, J., Alonso-Zárate, J., Verikoukis, C., Pérez-Neira, A. I., & Alonso, L. (2007). Cooperation on demand protocols for wireless networks. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*. <https://doi.org/10.1109/PIMRC.2007.4394100>
- Greenwood, D. (2021). Applying the principles of zero-trust architecture to protect sensitive and critical data. *Network Security*, 2021(6), 7–9.
- Hasan, M. M., Ibrahim, F., Mustapha, S. M., Islam, M. M., & Al Younus, M. A. (2018). The use of YouTube videos in learning English language skills at tertiary level in Bangladesh. *IUKL Res. J*, 6, 27–36.
- Li, D., Zhang, E., Lei, M., & Song, C. (2022). Zero trust in edge computing environment: a blockchain

- based practical scheme. *Mathematical Biosciences and Engineering*, 19(4), 4196–4216.
- Mehraj, S., & Banday, M. T. (2020). Establishing a Zero Trust Strategy in Cloud Computing Environment. *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 1–6. <https://doi.org/10.1109/ICCCI48352.2020.9104214>
- Mujib, M., & Sari, R. F. (2020). Performance Evaluation of Data Center Network with Network Micro-segmentation. *2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 27–32. <https://doi.org/10.1109/ICITEE49829.2020.9271749>
- Nyamasvisva, T. E., Atiff Abdalla Mahmoud Arabi, Buhari, A., & Wong, F. (2020). *Premeditated Academic Dishonesty : An IoT Based Preventive Solution*. (January 2021).
- Redondi, A., Chirico, M., Borsani, L., Cesana, M., & Tagliasacchi, M. (2013). An integrated system based on wireless sensor networks for patient monitoring, localization and tracking. *Ad Hoc Networks*, 11(1), 39–53.
- Rodigari, S., O’Shea, D., McCarthy, P., McCarry, M., & McSweeney, S. (2021). Performance Analysis of Zero-Trust multi-cloud. *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*, 730–732. <https://doi.org/10.1109/CLOUD53861.2021.00097>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (2nd Draft)*. National Institute of Standards and Technology.
- Sheikh, N., Pawar, M., & Lawrence, V. (2021). *Zero trust using Network Micro Segmentation*. <https://doi.org/10.1109/INCOMWVSHPS51825.2021.9484645>
- Sibghatullah H M, S., Elisha Tadiwa, N., Atiff Abdalla Mahmoud, A., Abudhahir, B., & Fares Anwar Salem, H. (2021). An Ad Hoc Movement Monitoring Algorithm for Indoor Tracking During Examinations. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(3), 3840–3846. <https://doi.org/10.17762/turcomat.v12i3.1672>
- Simpson, W. R., & Foltz, K. E. (2021). Maintaining zero trust with federation. *International Journal of Emerging Technology and Advanced Engineering*, 11(5), 17–32. https://doi.org/10.46338/IJETAE0521_03
- Sreeja, B., Saleem, M. B., & Sravya, V. (2020). Issues With Perimeter Based Network Security and a Better Model To Resolve Them. *European Journal of Molecular & Clinical Medicine*, 07(09), 2020. Retrieved from https://ejmcm.com/article_6830.html
- Stafford, V. A. (2020). Zero trust architecture. *NIST Special Publication*, 800, 207.
- Uctu, G., Alkan, M., Dogru, I. A., & Dorterler, M. (2019). Perimeter Network Security Solutions: A Survey. *3rd International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2019 - Proceedings*, (May 2020). <https://doi.org/10.1109/ISMSIT.2019.8932821>
- Uttecht, K. D. (2020). *Zero Trust (ZT) concepts for federal government architectures*. MASSACHUSETTS INST OF TECH LEXINGTON.
- Van Der Pol, R., Gijzen, B., Zuraniewski, P., Romão, D. F. C., & Kaat, M. (2016). Assessment of SDN technology for an easy-to-use VPN service. *Future Generation Computer Systems*, 56, 295–302. <https://doi.org/10.1016/j.future.2015.09.010>
- Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B. (2018). Access Control Policy Enforcement for Zero-Trust-Networking. *2018 29th Irish Signals and Systems Conference (ISSC)*, 1–6. <https://doi.org/10.1109/ISSC.2018.8585365>
- Wylde, A. (2021). Zero trust: Never trust, always verify. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–4. <https://doi.org/10.1109/CyberSA52016.2021.9478244>
- Xiaojian, Z., Liandong, C., Jie, F., Xiangqun, W., & Qi, W. (2021). Power IoT security protection architecture based on zero trust framework. *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, 166–170. IEEE.

WOMEN LEADERSHIP IN MALAYSIAN CREATIVE INDUSTRY

Kartini Kamalul Ariffin and Faridah Ibrahim
Infrastructure University Kuala Lumpur, MALAYSIA

ABSTRACT

This paper sets out to explore women leadership experiences and influences in the creative industry in Malaysia. Despite a growing number of researches focused on the leadership of professional working groups, with male leaders, in contrast research on women leadership has received little attention, what more in the new and upcoming creative industry. The Creative Industry refers to a range of economic activities which are concerned with the generation or exploitation of knowledge and information. They may variously also be referred to as the cultural industries covering 13 areas of activities namely advertising, architecture, the arts and antiques market, crafts, design, designer fashion, film, interactive leisure software, music, performing arts, publishing, software, television and radio. This paper narrows down the scope to women leaders working in film, digital, television and radio in Malaysia. With more and more women running the show in these sectors, there is a growing opportunity for women to control and influence the content in the programs. These women are not just industry leaders, they have the power to shape society's attitude. To understand the situation from the women leaders themselves, this paper using data from in-depth interviews, discussed the characteristics and contributing factors for women to rise as leaders in the creative media industry as well as their influence on content development and the extent of their decision-making prowess. The preliminary findings from four selected informants in this in-depth interview found that digital transformation plays a crucial role in giving a voice to women creators, and thus allowing them to create influence amongst their followers. When it comes to content creation, awareness and consciousness are heavily mentioned by both informants, it is concluded that despite effort to inject empowerment and break the cultural stereotypical mole of a women's role in the media, the effort is often diminished by popular culture, ratings and revenue. The audience acceptance is highly regarded, and often media houses will give them what they want. In order for women to rise as leaders, a support system is a secret recipe to their success.

Keywords:

Creative Industry, women's leaders, decision-making, broadcast, digital

INTRODUCTION

We could go to watch a film, spend Sunday afternoon watching your favourite soap operas on TV or be stuck in traffic while listening to your favourite radio station. Not mentioning scrolling your social media to find out about the latest news and finding recipes for dinner. We will most likely encounter a content or watch, listen and follow a woman showcasing her crafts on these platforms. While women make half of the world population, only 1 in 4 people heard or read about in news are women, only 21% are film makers and only 23% of film feature a female protagonist (UNwomen, 2020).

According to Beijing platform for action which turns twenty in 2020, cited that research spanning more than 100 countries found that 46 percent of news stories, in print, radio and television uphold gender stereotype. Behind the scenes, men still occupy 73 percent of top media management (UNWomen, 2018).

Along similar line, when gender relationship is concerned, the content of media, media language and visuals have the potential to accentuate the prominence and dominance of gender relationship and hence resulting in stereotypical gender generalisations (Strumska-Cylwik & Faridah 2014). These scholars also contended that media language and portrayal of content also play an

important role in creating social awareness that is associated with the opinions, beliefs and models of the way people think.

In year 2000, 189 UN Member States recognized the central role of media in shifting the gender stereotypes in the inaugural Beijing Platform for Action. Women and media are part of the 12 critical areas for action and urging media everywhere to make greater contribution to women's advancement.

The rise of women in leadership and political roles is positive but slow, and based on current trends, it could take another half a century to reach the UN Millennium Development Goals for Gender Equality in Political Representatives. Areas of agreement discussed during the conference are to increase number of women in media especially in decision making, abandoning stereotypes, training for women leaders, professional guidelines to reduce discrimination and establishing a watch group to track progress. Women in their own entities are different from men when it comes to their learning experiences and accumulation of knowledge (Khalid Mukhtar & Siti Maziha, 2017) and hence, have their own specialisation in contributing to nation building.

The purpose of this qualitative research is to examine the influence of women leadership in the creative media industries. Shanna Li et al. (2019) found in their study that leaders have a powerful influence on the expectation and behaviours of their followers from both male and female. Leaders inspire their followers to maximise their creativity which will then lead to empowerment. Hence, the focus of the present study is the question of Women leadership and Creative Media Industries in Malaysia. We pay particular attention to the creative industry because it has emerged as one of the new industry that holds a massive potential in boosting a nation's growth and income. The culture and creative industry is one of the world's most rapidly growing economic sectors. The economic contribution of the creative industry globally is widely acknowledged. It is estimated to represent anywhere from 3% to 12% of global GDP (World Economic Forum, 2014). This makes it a powerful emerging economic sector that is being strengthened by a surge in digitalization and services.

In Malaysia, the creative industry is rapidly growing into a lucrative and financially stable sector. Malaysia's rich culture and heritage is an ideal setting for many talented Malaysian to showcase their creativity especially women. In United Nation Conference in Trade and Development (UNCTD 2008) report, Malaysia has been identified as one of the top cultural producers among developing countries. In 2009 the creative industry have become a policy focus area of the Malaysian government, with the launch of Dasar Industri Kreatif Negara (DIKN) document in 2009.

In a time of rapid globalisation, many countries recognise that the combination of culture and commerce that the creative industries represents is a powerful way of providing a distinctive image of a country or a city, helping it to stand out from its competitors. Creative industries also help to shape and influence the public's mind.

With all that being said, how much of the creative industry represents a women's voice? Women's leadership and decision making in the creative industry is very crucial in order to give a fair representation of content, images and perception of the country to the world. This is very significant in the current situation where every global government is striving to achieve sustainability in their day-to-day dealings. Sustainability is a framework upon which specific strategies could be used to guide decision-making (Huda Ahmed Idris & Faridah, 2021). Sustainability suggests that in the decision making process societies have an obligation to ensure equalities and fairness for all, regardless of gender differences.

This qualitative study examined women's leadership role in the creative media industries in Malaysia specifically narrowing it to area of activities of television, radio and digital platform. Areas of which women have played a role in building the country's financial stability but not necessarily benefitted from the country's economic progress.

Objectives – In line with the purpose of this study, the following questions are formulated.

1. What are the characteristics and contributing factors for women to rise as leaders in the creative media industries?
2. How they influence content development and decision making?
3. What are the factors contributing to women under-representation in media leadership in Malaysia creative media industries?
4. What are the future strategies for women leaders in the creative industries?

METHODS

The selected research methodology for this paper is the Qualitative research design. A total of eight women who hold or recently hold leadership positions in creative media participated in an in-depth interview ranging from thirty minutes to one-hour long session. Informants selected are amongst those in senior leadership positions and have served the creative media industry for more than 10 years.

This study analyses data collected through a series of qualitative interviews. This study takes an applied research approach by contributing to the current field of knowledge around women leaders in creative media. It provides an improved understanding of the existing challenges for women and aims at beginning to identify areas for solutions to be developed. Thematic Content Analysis was used to analyse verbatim data from the interviews and elucidate common themes from the women's experiences.

This study, from its inception through analysis, took place between January 2021 and March 2022 in Kuala Lumpur, Malaysia. The interviews were conducted in various locations of the participants' choice. For this preliminary research, verbatim responses from **four** informants were extracted, out of the eight interviewed, to provide initial data for this paper. The interviews were conducted via online platform ZOOM due to the lock down.

Qualitative research has been valued because of its ability to provide depth information about a particular phenomenon. Qualitative Research is primarily exploratory research. Qualitative research generally includes data in the form of *words* rather than *numbers* (Punch, 2013). It is used to gain an understanding of underlying reasons, opinions, and motivations. It provides insights into the problem or helps to develop ideas or hypotheses for potential quantitative research. Qualitative Research is also used to uncover trends in thoughts and opinions, and dive deeper into the problem. Qualitative data collection methods vary using unstructured or semi-structured techniques. Some common methods include focus groups (group discussions), individual interviews, and participation/observations. The sample size is typically small, and respondents are selected to fulfil a given quota.

The researcher uses this method in order to find a deeper understanding of the situation based on the subjective individual experience which the researcher will analyse qualitatively. Qualitative methods are inclined to be looking at subject perspective or participant perspective. The qualitative method is used instead of a statistical approach which uses mathematical procedures because the aspirations and the experiences of the respondents are unique and diverse. Qualitative methods are naturalistic as they unfold naturally; non-manipulative and non-controlling; the researcher is open to whatever emerges.

The method is emergent and fluid as it accepts and adapts to inquiry as understanding deepens and/or situations change; the researcher avoids rigid designs that eliminate responding to opportunities to pursue new paths of discovery as they emerge (Silverman, 2016). Qualitative research is "information rich" and illuminative. That is, they offer useful manifestations of the phenomenon of interest; sampling is aimed at insight about the phenomenon, not empirical

generalization derived from a sample and applied to a population. To comprehend some meanings of life, one must get close to that life, (Stake & Jegatheesan, 2008).

ABOUT THE INFORMANTS

About the informants, three informants are business owners and founder of their production houses specialising in film, documentaries and content for television and one of the informant is working for one of the major media company in the country as one of the senior leadership team member. All of them have been in the industry for more than 15 years. The business owners are also producers and directors, they are known for their women empowerment content. All four informants are award winners in their own field

Informant 1 has started directing and producing since the early 1980's, informant 2 was a local Mass Communications graduate in the 90's, informant 3 started her career as a consultant in the financial field before entering the creative industry as a drama series writer and informant 4 started her career in advertising 20 years ago in an Oil and Gas company as an advertising assistant while studying for her Bar exams. After graduating from Law School, she joined a music label. Informant 1 has directed and produce nine well known films under her belt, informant 2 has produced more than 20 titles, of which some won international recognitions, informant 3 a writer, producer and director of popular Malay drama series for free to view channel and informant 4 was often sought after in an advisory role for new businesses, especially when it involved marketing to the urban youth and was involved in the set up and launch of a few radio and TV channels.

Their diversity as a director and producer works on diverse genres such as romance, soap opera, horror, and history, and is an explicit version of third-wave feminist consciousness embodied in a sarcastic sense of playfulness that feminist media studies cannot ignore.

FINDINGS AND DISCUSSIONS

This paper reports preliminary findings related to women's leadership in creative media industry in Malaysia. Based on the research questions they are grouped under four main themes:

The findings are based on **four** women leaders' personal narratives collected during the in-depth interviews.

Findings for RQ1

What are the characteristics and contributing factors for women to rise as leaders in the creative media industries?

For the **four** women leaders that was interviewed during these preliminary data collections, there were overlapping themes of common characteristics contributing to the rise of women leaders in the creative media industries from their interview. All the informants have been involved in the industry for more than 20 years, and have experience the changing landscape of the creative media industry - from traditional platform to digital transformation. Themes that emerges from this research question are – ***Digital Platform, Entrepreneurship, Support, Gender Consciousness and Opportunities.***

Digital Platform

They strongly agreed that the rise of technology enabling democratisation of broadcast platform has given opportunity for content creators to share their voice. Women influencers are gaining control of their content and appear authentic and genuine as compared to the traditional platform. The demand

for content and the rise of every person on social media was further amplified by the lockdown as a result of the pandemic.

Lockdowns resulted in increasing social media usage, a shift in customer behaviour from Covid-19, production issues with traditional advertising shoots, audiences gravitating toward authenticity and curated content, and brand budgets being upended, necessitating the swift change. Informant 2 summarises her view by saying that:

“So I think there is... there has been a shift. And I think the influence because of the fact that women are willing to voice up and using social media and in the more mass media space”
(Informant 2)

In addition, informant 2 observed that the digital space embraces the freedom of expression in a new liberating way. With lower cost of entry and less stringent monitoring by the authority, almost anyone with the passion to create content has the opportunity to rise. Furthermore, all the aspects of editorial decision are determined by the creator, they decide what should be broadcast.

“Well basically all these women are saying to hell will all this authority lah... aku nak buat sendiri, it’s a question of survival you know so when it comes to survival, they seem to be able to handle it” (Informant 2)

The digital space presents women creators with a platform that is accessible, cost effective and user friendly. The digital realm has created a value system where women are no longer forced to stay within the concept of socially acceptable femininity. Moreover, their efforts to break these limits and express their authentic self are financially and materially rewarded.

Informant 3 highlighted that stamina is key in sustaining in this industry, it does not matter what your gender is. With the internet of things, there so much opportunities to be discovered, and resourcefulness is an essential trait.

“resourcefulness to manage themselves in this industry to make them last longer because it’s about whether they have what’s the energy” (informant 3)

According to a research by Idahash International Influencer Report 2017, women - rule social media, influence purchase decisions, set trends. According to our study 68% of social media influencers are female. Thus is echo’s the sentiment of the Informant 4 that opportunity is key in encouraging more women to play the leadership role, and this is what the digital platform offers, and opportunity for anyone to thrive.

“...if you don't create that opportunity in the first place you wouldn't find someone qualified”
(informant 4)

Entrepreneurship

The informants also highlighted the fact that entrepreneurship plays an important factor in encouraging the rise of women leaders in the creative industry. Three of the informants are business owners and they are founders of their own production company. Thus, this set up has allowed them to have control of almost all aspects of their company, products, content and services. Being a business owner liberates women from the typical hierarchal corporate world. Bendell et al. (2019) claim that female entrepreneurs have significantly higher self-leadership skills.

Abd Rani (2018) has stated that due to the patriarchal structure of Malay families, the need for self-identification and achievement among women has encouraged the large-scale participation of

women in such fields. This means that the patriarchal system and male dominance have emerged out as a regressive system enabling women to take creative industries as a way of proving their identities. Creative industries are generally more receptive towards soft skills such as community building, networking, and writing as opposed to hard skills, which require complex problem-solving techniques (Sopa et al. 2020). This makes a case for women, who in Malaysia are mostly confined to their homes, are expected to take up creative industries more than their male counterparts.

Informant 1 stated that,

“I see a lot more women creators who do um... produce, create own content and they run their company, they try to do different things you know” (Informant 1)

While informant 2 contributes the rise of women business owners to the advancement of technology and the open-ness of the digital space and allows entrepreneurial mindset to thrive.

“ The mushrooming of business using live streaming um digital business using digital platform... so things are grown in more ways that you can imagine . We call it the punca kuasa, you’re the power” (Informant 2)

The study of Sanyu (2018) has cited globalization along with technology as the main drivers of this change. This is because, with the technology, women do not have to work at a physical location but can now work anywhere with a stable internet connection. This gives rise to women entrepreneur amongst women especially opening business from home selling online.

Informant 3, opines that for a women to be holding the highest position in a production set , the chances of her to be the director in charge, is much higher is she owns the company. Which means that her chances of pitching and winning the position is higher.

“ if you want to be a director, you have to come up with your own company , Unless you are appointed” (informant 3)

Support

A superior support can help and employee increased job satisfaction, improved relationship with employees, increased organisational citizenship behaviour and reduced job tension. The interviewees both agreed that without the recommendation and strong support from leader or direct supervisory personnel, the chances of an employee to rise to leadership position is weaker. What more for women a superior who advocate for her promotion give her a better change to lead, giving her credibility and gaining the trust of others on her capabilities.

According to a research done by Fairygodboss and Female Quotient and Progyny (2018) to get a better understanding of the key differences between men and women when it comes to work and home life on 400 respondents, they found that men are more likely to be promoted by men, and women are more likely to be promoted by women. When speaking to informant 1, she is constantly aware when building her team. She is a strong advocate for women to take the lead, but found it challenging to find women who wants to take on the position.

“I’ve tried so hard to find women female directors that I want to give projects to, nak bagi tau. Like I can't find... I can't find!!! and then the ones that are already directing, they're directing, they're busy. “(Informant 1)

Informant 2 shared her observation on women leadership role in public broadcasting. She observed that in the government sector the political influence played such an important role. A change in government would also mean a change in the senior leadership team.

“Sometimes you depend on the minister, the minister likes you or wants you to stay, then you stay lah, if not then you get transferred out, so and, but you know it makes a lot of difference when you have women in charge”.

(Informant 2)

Informant 2 also highlighted that women especially those who are empowered and gender sensitive will ensure that women are promoted positively. Despite the challenges that they face with the stereotypical demand of broadcaster, women will fight for women to be in the main lead.

“In my team my company mostly the women, the one that’s very active in promoting content that have women as in the lead characters uh even though like the tv station state that they want women yang abcd ... a bit more the typical lah but we always try and push” (Informant 2).

Informant 3 argues that, when it comes to women advancing her career in the creative industry it’s all about the ideas. It does not matter what the gender is as long as the idea is valid and interesting, then the person will be able to sustain and garner support from their superiors and colleagues.

“it’s about ideas who I mean it’s about um you know in the end of the day who can last long is the ones who have ideas and uh not just the ideas but also um the resourcefulness to manage themselves in this industry to make them last longer because it’s about you know whether they have the energy” (Informant 3)

Interestingly informant 4 raised about the openness of male employees to work and accept a female boss. Without such shift in mindset and culture, the rise of women in leadership within the industry may be challenged.

“it was actually quite commendable that he actually respected the fact he could have female boss, so that chemistry need happen in any transition or in any the industry right, to have given and take because not all men said, oh I can give in this position” (Informant 4)

She also cited that 20% increase in women leaders, contributed by various factors not limited to male colleagues support and acceptance.

“Today what I see in the creative industry, that a lot of women have gone up became the GM, see level and they even hold the top position in creativity and so now it use be maybe 20% women involved” (informant 4)

In order for women to succeed and stay in the workforce, her family support system must be in place. Family and motherhood are top priorities for working mothers, and when the family is taken care off, she can perform better at work.

“ they forget to realise when women have peace, they can even contribute better they have to be really strong and also have good support system within the family whether they have the in law to stay back ...or good day care or supportive spouse like that’s it really important but it still not every women is fortunate enough to have” (informant 4)

The fact that not every women is privileged to have a conducive family support system due to it's individual and per case basis, women fall out on the opportunity to even stay in the work force, what more reach senior leadership role as they are made to choose between family or career.

Mothers especially may experience strong feelings of guilt for having career aspirations (Guendouzi, 2006). Despite the apparent gender-neutrality of parenthood demands, they remain highly gendered; caring is still primarily seen as the mother's task (Bowlby et al., 2010).

Gender consciousness

Gender consciousness aims at increasing general sensitivity, understanding and knowledge about gender (in) equality. Awareness raising is a process which helps to facilitate the exchange of ideas, improve mutual understanding and develop competencies and skills necessary for societal change (Strumska-Cylwik & Faridah, 2014). These scholars argued that awareness raising comes with great challenges where media messages connected to gender are often subjected to some interpretation subordinated to specified ideologies, political and cultural habitus that given opinions and linguistic patterns connected with gender are based on.

Nevertheless, with greater gender sensitivity and more exposure to knowledge in the current evolving societies brought by globalisation, we are now more gender conscious than before with the available excess to resources on the internet, open conversations and discussions on gender equality, there's much more exposure and awareness amongst the public.

Informant 2 attributes the rise of women leaders in the creative industry to this, the gender consciousness movement are visibly and accessibly to anyone, and thus men are equally exposed to it too. She opinionated that it doesn't matter if they are men or women, but they need to be gender sensitive to make that change.

“if they are not gender-sensitive, they will never be able to make that difference” (Informant 2).

Informant 1 observed the shift throughout her 20 years' experience being in the creative industry, there is an uprise trend.

“And I think the uh the voices of the women producers the women creatives are getting very loud, So I I mean I feel yes there is a bridge, there is a change, there is a shift” (Informant 1)

Informant 3, strongly feels that anyone can be a leader, regardless of gender, it's all about inspiring and positivity, a good leaders does not discriminate and will aspire to do what is right and this includes gender equality. Thus informant 3 opines that a good leader is gender conscious regardless if it's a man or woman.

“ I think in terms of leadership, it's really individual. I mean again la, to me, there's no gender I mean if somebody has leadership skills, then therefore they will lead effectively, and it depends on how much they can inspire. ” (Informant 3)

Informant 4, opines that women leaders does not necessarily have a higher gender consciousness, from her own personal experience, a female boss can be as insensitive.

“I have female boss also the strong career women and she elderly, she like a man, she behave like a man actually and try to run the business like a man, and it also she very brave, she said things like ah yow, you pregnant ah. You know she doesn't have kids and she doesn't see that, even the male boss wouldn't say the things like “ (informant 4)

Findings for RQ2

How they influence content development and decision making in content creation?

Themes that emerges from this research question are – *Revenue vs Ratings, Pushing Boundaries, Balancing cultural sensitivity.*

Revenue vs Ratings

Informants are clear on their sentiment towards women portrayal in the creations. Be it from screening strong positive women lead roles to the people who are working in production. They make a conscious decision to hiring women to take the lead.

On content development all informants are very involved in conceptualising the story of their end product be it a full length film or for television programs for broadcasts. They are involved from the beginning of the inception of the project, from selecting the writers, actors, producers, directors right up to the production crew.

An interesting insight from informant 1, 2 and 3 informants regarding content creations is the fact that even though they are advocates of breaking the stereotypical portrayal of women in media, they have to understand the mindset and acceptance of the viewers. The ratings which then results to revenue is a very important indicator for any programs to be broadcasts. Informant 1 exclaims that,

“Open advertising that decides. you can have a parent power woman out there but the moment you are driven by your advertising needs you no longer the influence that we can rely on” (Informant 1)

Informant 2 on the other hand highlighted that, even though the creators included a slight tweak in the storyline to show an empowered women character, the cultural norm may resist it, forcing creators to go back to popular culture.

“And then Datuk said um itu kita buat and then we sold and then no lah ratings tak bagus, Diorang tak boleh accept she ran away” (Informant 2)

This sentiment also arised from informant 1, when she shared

“...even women don't want to see characters kalau perempuan tu too strong they want you to tempo it down a bit” (Informant 1)

Informant 3, highlighted that as much as she consciously portrays her women characters positively, she ensures that what she writes reflects reality,

“I will write according to what I see. So contohnya macam I feel that nowadays there are more women leaders in a family unit, so I will write that. So macam contohnya some women are the breadwinners, so I will write things like yang touch on reality-based “ (informant 3)

Striking a balance between popularity and women empowerment content is a challenge for local producers, where cultural norm and patriarchy system dominates the society's mindset. Though there's much awareness and effort on the creator side, the acceptance of the general public is still low. The audience expects an ending that is expected and accepted

Pushing Boundaries

When it comes to content, the two informants who are respected figures in the film and drama industry, shared that they have to push the envelope in their quest to influence content creation. They would recruit like-minded group of people to work on the project. Informant 2 shared that,

“When I create stories I always make sure that I want some of the characters or the main character to be more substance and for me that is an important thing and the people who work around me, writers who collaborate with me they share the same sentiment so it’s easy”
(Informant 2)

Informants 1 and 2 also shared that they mentor and coach other team members to think critically and look at how content can create impact.

“I’m sharing something that can inspire them to think beyond on what you can do and to be helpful to your own gender not just your family your friends but there’re women out there who genuinely needs help” (Informant 1)

Despite been given a predictable brief by clients or stations when it comes to content, informant 1 is a rebel when ensuring that the women agenda is taken seriously.

“in my team my company mostly the women... the one that’s very active in promoting content that have women as in the lead characters uh even though like the tv station state that they want women yang abcd ...a bit more the typical lah but we always try and push” (Informant 1)

Working creatively around the norm, manoeuvring within boundaries, but yet need to inject elements where audience are triggered to think.

“when I convince them that it’s in your hands to then change it to make it interesting without losing what is good about the novel” (Informant 2)

Informant 3 and 4, does not feel that they need to push the envelope far, as what they are portraying in their writing and content is already reflecting close to reality.

“...writers they write, it’s based on what what they feel that is culturally correct. I will write according to what I see. So contohnya macam I feel that nowadays there are more women leaders in a family unit, so I will write that.” (Informant 3)

Informant 4, sees an acceptance for strong and heroic women characters. There’s an appeal to see positive, unconventional women roles.

“I think they (men) celebrate the fact that women, you know last time was portrayed in the very feminine way but now they portrayed as more heroic. I think and men in general support that and in fact they celebrate and find sexy and appealing” (Informant 4)

Informants 3 feels that the reason for this acceptance is because of the strong respect mothers received due to cultural and religious reason. Many culture in Asia are matriarch and mothers are placed on the pedestal, their voice matters and they make important decision making in the family.

“So you know when your mom especially kat Malaysia, orang Melayu kan I mean they say lah mak is apa...kalau nak masuk syurga you have to cium tapak kaki mak, the mom is like the mother is like the biggest thing in in Muslim Malay culture kan” (Informant 3

The quest to influence or create change in breaking the stereotypical role of women as seen in our media is not an easy one for informants 1 and 2. Despite being someone of power, dominance and influence with a cause, they have to push and persuade. Informant 3 and 4 on the other hand observes that there's a wide acceptance and demand to see positive and strong women characters in our media, but they must be within cultural context.

Balancing cultural sensitivity

Cultural sensitivity refers to a set of skills that allows you to learn about and understand people whose cultural background is not the same as yours. In the content creation context, all the informants are aware that their culture and gender view may not be similar to the target audience. Our informants, may come from the educated, English speaking and a diverse background from the originally intended audience.

“ It's a catch-22 where the tv station wants the character to be like this, you know you have the story but they want a woman who is like a cry baby or a whinner because they say people want to see characters like that, the audience don't want to see strong woman people in charge of programming tv station themselves are not sensitive towards these needs maybe there are but they don't have a voice in there” (informant 1)

From her experience adapting a popular novel for television, her writers highlighted on how the novel conforms to women stereotypical characters, and predictable storyline. In their effort to balance the cultural sensitivity of the intended audience, they carefully crafted plots and characters that's empowering.

“when I convince them that it's in your hands to then change it to make it interesting without losing what is good about the novel” (informant 2)

Informant 3 noted that women who are taking the lead in their family and becomes the main financial provider for the family, they still plays very strongly her culturally assigned role, despite being the income producer.

“I know this family lah the woman is the breadwinner, the husband is the house husband but the woman still respects the husband like like he's the leader of the family and then and he but he takes on the role and they cooperate tau” (informant 3)

Informant 3 also adds on that audience accepts the role reversal concept, and it is accepted for the men not execute his society's imposed duties and take on the women's duties

“In this drama I wrote, the character is a good house husband so he cooks, So takde issue, and then we put comedy we insert comedy in it, so it becomes like a laughable matter” (informant 3)

As the nation progresses, Informant 4 attributes that the society is more open to acceptance

role reversal between men and women. As families shift into this non-traditional provider role, there are significant changes in the families' home role, where there is an increased presence of men in fathering roles that challenge traditional expectations (Rochlen, Suizzo, McKelley, & Scaringi, 2008)

"Because we don't judge them, if you said you are a house husband like oh my god we tabik you, because you amazing, because your ego is not shattered, it also the change in the society in accepting that women have to go work and men need to stay back look after the kids and do house chores." (informant 4)

Findings for RQ3

What are the factors contributing to women under-representation in creative media industry in Malaysia.

Themes that emerges from this research question are – *Cultural and institutional barriers, The Confidence Gap, family commitments and motherhood*

Cultural and institutional barriers

For informants 1 and 2, culture has been heavily highlighted as the main factor in contributing to women under-representation in creative media. The stereotypical perception of what a woman should be still prevails in the society's mindset despite the fact that a woman may hold credentials, experience and leadership role. In various occasion informant 1 shared that she resorted to getting a man to represent her views in order to get buy in, especially when highlighting sensitive gender issues.

"but I've had times when I pass a paper to my male colleague can you bring this up I think if I bring it up it will be sensitive" (Informant 1)

Informant 2 add on that people find that when a woman speaks or leads and tries to insert a change they are seen as though they have a hidden agenda.

"Whereas I think if a man speaks up somehow people listen to it more. If a woman's talking about it, can we make the woman character macam ni macam ni, people be like eh apa your agenda ni feminist ke..." (Informant 2)

Women leaders are still minority amongst the pool of men in the creative media industry Malaysia. Thus, lacking in support and sense of belonging makes being a female lead a lonely journey. Women are expected to behave and join their male counterparts, and this can be very discouraging and demotivating, this is what informant 1 has to say about Boys Club;

"in the bro club you either the teh tarik club go to uh warung with the guys or you're drinking club go drinking with your bosses or your guys which you know you can't fit in there" (Informant 1)

Informant 2 echoed the sentiment and added that because we see leadership as a very masculine role and in a patriarchal society, woman is seen as nurturing, obedient and are expected to behave in a certain way, placing a lot of pressure for women to conform.

"And I think there's a lot of pressure because for especially women uh, and more so actually especially Muslim women because they're so more judged than any other you know. So it's a

lot more pressure to be ...to be good... good on the internet than... than to be different”
(Informant 2)

Informant 4 shares her experience that she felt the pressure to conform to the stereotypical idea of masculine leadership. It was not only reflected thru her action but also to the clothes she wears to office.

“ I need to wear pants to work, I still wear whatever I want to go to work but I only wear pants to work maybe, subconscious that I need to behave to everyone before I get accepted into that group. So I wore pants, only pants and I never had a dress or skirt that I wear to work. Maybe for the subconscious, if I wear that, I will be weak” (informant 4)

And because of this cultural mindset, informant 3 takes a different approach and instead of trying to impose change, her writing glorifies the women’s conventional role. The messaging that a women chooses the role that she wants to play and it does not mean that she is weak just because she choose to retain in a traditional setting.

“I wanted to portray is it's okay to be a housewife, don't look down on suri rumah tangga we wanted to show that that that it's okay to have these traditional roles but everybody has to play an equal part in the traditional role.” (informant 3)

The cultural mindset posts a challenge for women to rise as leaders in creative media industries. Though they may bring in their own leadership style and strengths, she may be seen as ineffective because what we are used to seeing and experiencing is the masculine style which tend towards assertive and tasks base behaviour. Women’s leadership style is more relationship oriented and democratic.

The Confidence Gap

A study done at Cornell University by David Dunning and Joyce Erlinger (2003) found that men overestimate their abilities and performance, while women underestimate both. In fact, their actual performance does not differ in quality or quantity. The informants highlighted the same sentiment thru their experiences, they highlighted the level of confidence that men displayed are much higher than their counterpart. According to informant 2, when offering jobs opportunities such as directing a film,

“Guys were like, yes okay I’ll do it like oh can I can you give me to me I will I want to do it.”
When we tell the girls to say how about trying to write, how about trying to direct... they may have to think can I can I can I do this... I don't know whether I can or maybe I'm not creative enough” (Informant 2)

As a result of this lack of confidence women does not pursue future opportunities, and thus hiring women into the industry a challenge. Informant 1 shared about her search in hiring women directors, where the she wanted the position to be held by women, but found it challenging to fill.

“ I can’t get the girls or maybe the girls just feel like we do our own thing which also happens, I asked sometimes they said no lah no lah we’re not ready lah, we do first our small small little production.” (Informant 1)

On top of that informant 2 shared that women fear rejection and disappointment more than men.

It's the I would say confidence, what is the macam like like the muka tebal la. I don't know whether for guys they they don't worry about so much about rejection you know, they'll come out and they're like like like yeah direct for you lah. (Informant 2)

Informant 4, opined that women are not encouraged to be their authentic self, women feels the pressure to not optimised their feminine traits when it comes to leadership. This results to confident gap, when an individual have to emulate a persona which they are not.

“women end up in senior position they tend to speak the language or the way man does, let say you are in C level you're expected to man up, wears the pants” (informant 4)

Family and motherhood penalty

New research proves that "motherhood penalties" are real. According to the latest annual Bright Horizons Modern Family Index, 69% of American workers say that working mothers are more likely to take over new jobs than other employees. 60% say career opportunities are given to less qualified employees rather than qualified working mothers 72% of working mothers and fathers agree that women are at a disadvantage in their careers to start a family, while men are not.

While Informant 1 and 2 did not state family and motherhood as a barrier for women perhaps because they are single women, informant 4, who is a mother of two, cited strongly that family commitments does get in the way for women to progress in their career.

“ women not given the opportunity to shine because when they about to make their break they have family commitment, and they kind drop off along the way, a lot of them don't go on to push further to making to the top. That's very apparent, I don't know whether this is just creative industry but most the industry they do that, family come first “(informant 4)

Informant 3, though unmarried, noticed the motherhood amongst her peers and circles.

“that's the kind of challenges that that any woman would face now. When there's motherhood and when it comes to family especially orang perempuan yang the ones that have to care” (informant 3)

Gender and family studies have long shown that parenting has different effects on women's and men's income. Women usually experience wage cuts with the birth of each child (Budig and England 2001; Gangl and Ziefle 2009; Gough and Noonan 2013; Yu and Kuo 2017). For example, one of the reasons that becoming a parent increases a man's income and reduces a woman's income is that it motivates men to take care of their families, but reduces the time and energy available to women for work. (Budig and England 2001; Gough and Noonan 2013; Killewald 2013).

Findings for RQ4

What are the future strategies for women leaders in the creative industries?

Themes that emerges from this research question are – *Education, Policy, Flexibility*

Education

When women come to power, everyone benefits. According to the Westminster Foundation for Democracy, this leads to better results for society as a whole, especially in areas such as health, infrastructure and education. Therefore, women empowered with have a role to play in advancing

education, but the relationship is not one-sided. In fact, education is an important tool for empowering women. This was fully agreed by informant 1 who suggested that

“so I think it’s timely we have that, then there’s a lot of things that can be done, even under one roof you can work towards women empowerment their development starting with the education first discussing empowering women through having a women university or a university for women” (Informant 1)

When mentioned education, it’s not only limited to formal education, but creating awareness by initiating conversation surrounding the topic, as per informant 2.

“...there has to be more these kind of conversations that take place at very high levels at leadership levels “(Informant 2)

The need to create awareness about the different jobs and roles, and to expose more women to the roles that they wouldn’t normally pursue,

“think that there should be more women directors like myself. I don’t think that women do. There’s not a lot of women directors in the industry” (informant 3)

This is then echoed by informant 4,

“there always the guy who walking on the studio, there always the guy right and even the production are usually the guy and women are just the script writers and the talent “(informant 4)

Policy

There is a need for policy and program activities that raise awareness through effective education, media programs, outreach programs, discussions and more. Though many parties believe that organic method without intervention is an ideal way to move forward, but without and policy change this progress can be stagnant and sluggish. Informant 1 highlighted that,

“so there’s some good women but because your policy such that when you change you want people in your party to come in then you rather take people who are unqualified, not suitable but as long as it fulfils your um political needs, so it affects the development of a lot of things but in the creative industry it is badly affected when you start doing that” (Informant 1)

While informant 2 is in an opinion that because we have lack of awareness in the area, it’s hard for people to be aware, most of the time they are oblivious to their choices. Thus, if there’s a policy imposed, people would be more conscious

“I think what we are not doing is we’re not being conscious enough , for example we have a panel, mesti ada kalau kita say okay we are talking to Malaysian directors, and then on the panel and all Malaysian directors are same race, same gender” (Informant 2)

While Informant 3 agrees,

“I think you should have equally men and women working together and I you know the the government has to impose that you know...the equal” (informant 3)

Thought imposing policy a mean of intervention, might be debatable, but policies and procedures provide a road map for change. They ensure compliance with laws and regulations, give guidance for decision-making, and streamline processes.

Flexibility

Flexitime is a practical model that focuses on achieving greater deadlines and goals than the rigor of the 9 to 5 schedule and when and where things happen. As long as the employee is performing his or her duties, it can be anywhere. In the flexitime model, good communication between employees and managers is the key to ensuring that all team members understand what and when. Informant 4 is a believer of this and feels that flexibility in time and communications helps women manage career and motherhood.

“I actually a bit more sensitive throughout them, actually I give more flexibility to work from home or help them find or recommend baby silter nearby or give them more time to settle down, if we not settle at home and we never be settle at work. So since I had kids I am actually more responsible in that sense or more sensitive to women.” (informant 4)

Informant 2 opined that, women too needs to be flexible and open to change. While a more condusive working hours and environment is put in place, women need to want the career progression.

“And I think if the women want to see change, they have to step up too.” (informant 2)

CONCLUSIONS

This paper discussed the challenges and potentials of women leadership in the media creative industries. To understand the situation, the characteristics and contributing factors for women to rise as leaders and their influence on content development. The discussions are based on the in-depth interview carry out amongst seasoned women leaders in the creative industry in Malaysia. Most respondent attributes areas such as support, entrepreneurship, digital transformation and gender consciousness as crucial in paving the way for women to rise in leadership. In term of conceptualising content – creativity, consciousness and pushing boundaries while balancing cultural sensitivity are some of the ways where they exert their influence. When it comes to women potential, informants believed that women have the prospects to go beyond. Only if aspects such as policy, education and flexibility are considered seriously by the industry and the governing body to see women’s contribution as leaders in the creative media industry.

The context of this may not fall into the stereotypical definition of corporate leadership, but these women are leaders, where they speak up their minds and give a voice to others. When it comes to content creation, awareness and consciousness are heavily mentioned in the study, it is concluded that despite effort to inject empowerment and break the cultural stereotypical mole of a women’s role in the media, the effort is often diminished by popular culture, ratings and revenue. The audience acceptance is highly regarded, and often media houses will give them what they want. In order for women to rise as leaders, a support system is a secret recipe to their success. Having superior’s buy in and recommendations goes a long way to seeing a women climb the file to rank of the creative media industries.

AUTHOR BIOGRAPHY

Kartini Kamalul Ariffin is a Doctoral student at the Department of Communication, Faculty of Business, Information and Human Sciences, Infrastructure University Kuala Lumpur. She is currently a professional and a Managing Director in a digital media industry. *Email: kartini.ariffin@gmail.com*

Faridah Ibrahim, PhD is Professor in Journalism and Communication at the Department of Communication, Faculty of Business, Information and Human Sciences, IUKL. She has been in the academia for 35 years and was a professional journalist before joining the universities, UKM and IUKL. Her vast areas of research and publications cover war and peace journalism, organizational communication, film and broadcasting, media ethics and professionalism, and women in the media. *Email: faridah@iukl.edu.my*

REFERENCES

- Barsade, S. (2005). *The 'Masculine' and 'Feminine' Sides of Leadership and Culture: Perception vs. Reality*. Knowledge at Wharton, A business journal from the Wharton School of the University of Pennsylvania. <https://knowledge.wharton.upenn.edu/article/the-masculine-and-feminine-sides-of-leadership-and-culture-perception-vs-reality/>
- Bendell, B., Sullivan, M. & Marvel, R. (2019). A Gender-Aware Study of Self-Leadership Strategies among High-Growth Entrepreneurs. *Journal of Small Business Management*, 57(2), 110-130.
- Erlinger, J. & Dunning, D. (2003). *Why People Fail to Recognize Their Own Incompetence*. SAGE Book
- EU Business School. (2021). *How Education Plays a Role in the Empowerment of Women*. <https://www.euruni.edu/blog/how-education-plays-a-role-in-the-empowerment-of-women/>
- Fairygod boss Female Quotient and Progyny (2018). *Men and Women on Career Home Life*. Fairygodboss
- Flew, T. (2012). *The Creative Industry: Culture & Policy*. SAGE Books.
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5675340/>
<https://www.diva-portal.org/smash/get/diva2:1633192/FULLTEXT01.pdf>
https://www.researchgate.net/publication/233139860_The_role_of_gender_consciousness_in_challenging_patriarchy/link/02e7e521f4e3697091000000/download
<https://discovercorps.com/blog/cultural-sensitivity-awareness/>
<https://www.washingtonpost.com/business/2022/04/21/single-women-workplace-penalty/>
https://www.brighthorizons.com/-/media/BH-New/Newsroom/MediaKit/MFI_2018_Report_FINAL.ashx
- Huda Ahmed Idris Mohamed & Faridah Ibrahim. (2021). Sustainability and ethical considerations during the COVID 19 Pandemic. *International Journal of Infrastructure Research and Management (IJIRM)*, Vol 9 (1) June 2021, pp 62-70.
- Kay, K. & Shipman, C. (2014). *The Confidence Gap*. <https://www.theatlantic.com/magazine/archive/2014/05/the-confidence-gap/359815/>
- Kementerian Penerangan dan Komunikasi Malaysia (2009). *Dasar Industri Kreatif Negara*. Percetakan Negara.
- Khalid Mukhtar Othman Tawir & Siti Mazih Mustapha. (2017). Learning styles preferences, gender and English Language performance of EFL Libyan Secondary School students in Malaysia. *IUKL Research Journal*, Vol. 5 (1) 2017, pp 50-62.

- Punch, K (2013). *Introduction to Social Research: Quantitative and Qualitative Approaches*. SAGE
- Rushing, C., & Sparks, M. (2017). The Mother's Perspective: Factors Considered When Choosing to Enter a Stay-at-Home Father and Working Mother Relationship. *American journal of men's health*, 11(4), 1260–1268. <https://doi.org/10.1177/1557988317693347>
- Sanyu, A. M. (2018). New media, diasporic identity and social exclusion: A study of everyday practices of identity negotiation among second-generation Ghanaian women in Hamburg. *Crossings: Journal of Migration & Culture*, 9(1), 29-43.
- Shanna Li, Faridah Ibrahim & Siti Maziha Mustapha. (2019). Factors contributing to Organisational Climate: Evidences from Small Medium Enterprises in China. *IUKL Research Journal*, Vol 7 (2), 2019, pp 73-82.
- Silverman. D (2016). *Qualitative Research*. SAGE
- Stake. R and Jegatheesan.B (2008). *Access, A Zone of Comprehension, and Intrusion*. Emerald Group Publishing Limited.
- Strumska-Cylwik, L. & Faridah Ibrahim. (2014). Gender relationship and media language: A comparative study of print media in Poland and Malaysia. *International Journal of Arts and Sciences*. Vol.7(5): 647-682.
- Sopa, A., Asbari, M., Purwanto, A., Santoso, P. B., Mustofa, D. H., Maesaroh, S., & Primahendra, R. (2020). Hard skills versus soft skills: Which are more important for Indonesian employees innovation capability. *International Journal of Control and Automation*, 13(2), 156-175.
- The Commonwealth. (2015). Strategies for Increased Participation of Women in Leadership Across the Commonwealth. <https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/inline/Women%20in%20Leadership%20Discussion%20Paper.pdf>
- UNwomen. (2020) *Annual Report*. United Nations.
- UNCTD. (2008). *Creative Economy Report*. United Nations.
https://labs.indahash.com/wp-content/uploads/2017/06/indaHash_LABS_report_2017.pdf
- Wei-hsin Yu, Yuko Hara; Motherhood Penalties and Fatherhood Premiums: Effects of Parenthood on Earnings Growth Within and Across Firms. *Demography* 1 February 2021; 58 (1): 247–272. doi: <https://doi.org/10.1215/00703370-8917608>
- World Economic Forum. (2014). *Global Gender Report Gap*. UNESCO.
- Zenger, J. (2018). *The Confidence Gap in Men and Women: Why It Matters and How to Overcome It*. <https://www.forbes.com/sites/jackzenger/2018/04/08/the-confidence-gap-in-men-and-women-why-it-matters-and-how-to-overcome-it/?sh=6c7f73aa3bfa>

PRESERVATION OF ARCHITECTURAL MODEL INTO 3 DIMENSIONAL DIGITAL FORM WITH THE METHODS OF PHOTOGRAMMETRY

Adil Farizal Md Rashid, Rizal Husin and Md Pilus Md Noor
Infrastructure University Kuala Lumpur, MALAYSIA

ABSTRACT

Physical architectural presentation model is one of the most important mediums prepared by architects in order to provide a good immersion of visualized architectural details and massing of an architectural project. Ideally, good quality of physical architectural presentation models are done using a very high precision in detail, from the cuttings of the model to the small details of leaves in the scaled presentation model.

Unfortunately, these physical models throughout time will deteriorate, losing its pristineness and finally have to be thrown into the garbage after a period of use. The cost of a single-scaled model can reach up to hundreds or thousands of ringgit if it is properly done and well made. Because physical models normally consume a lot of space, such as galleries or storerooms. Most of the older or non-important models are thrown away or recycled. In this research and implementation of the technology called 'photogrammetry', we find that it is a good idea to preserve these physical models into a digital 3 dimensional (3D) model instead of a photograph physical model. It has its distinctive advantages over normal portfolios by architects especially for job hunters in the same field. It is to show off their skills and talent in preserving their works in a digital format that are more impressive than common portfolios. Indirectly, photogrammetry methods are expected to drastically increase the immersiveness of a project than typical project presentation in boards and actual models.

The methods are to use digital hi-resolution camera (minimum of 5 megapixel) and to take as much as 60 to 70 percent overlapping images (minimum of 40 images) from elevations, top view and 360 degree of scaled architectural model and analysing it using photogrammetry generating software to develop the 3d mesh. From the 3d mesh, animations, simulations and even 3D orbit visualization of the model can be preserved and used for future needs such as presentations or analysis.

This method hasn't been applied to any architectural institution in Malaysia yet and it is one of the initiatives to preserve architectural models, whatever the quality is, as it has sentimental value for its designer. It is hoped that this method can be developed into a more comprehensive and easier equipment for these research objectives.

Keywords:

Architecture, Education, 3D Visualization, Modelling, Animation

INTRODUCTION

Architecture education has been discussed and improved throughout time by educators and practitioners all around the globe. Due to the NATIONAL POLICY ON INDUSTRY 4.01 announced by the government in 2018, it is crucial that by 2030 all digitalization in industries and education institutions will excel in every aspect. This includes how education and delivery of databases can be properly managed and make it accessible to all.

The education and architectural archive can be improved by using the new and latest technology of photogrammetry that is accessible to most modern devices available now such as digital smartphones with cameras, photography kits and sets and also softwares that can process the data. It has become a need now for almost everyone to have their own personal smartphone that can be used to scan and analyse any physical architectural model into 3 Dimensional data that can be preserved for future needs such as portfolio, architectural database (archive) and precedent study.

Physical architectural models done by architectural students through time will tend to deteriorate and become damaged. These models also need to use a lot of space within any facility or accommodation acquired by the students or the faculty itself. This will also increase the cost of renting or maintaining the space for these models. Perhaps only the exceptional models that are very important and impressive will be shown as exhibits. The need for more space to place all these models eventually will accumulate a large amount of spaces including its circulation for the exhibition.

Therefore, with the platform of photogrammetry that is accessible and affordable, it is believed that it will work to improve the collection of preserved architectural models into 3D form that can be stored in physical drive or cloud storage for future references. It is crucial for institutions such as architectural schools to acquire such technology for the sake of keeping all the data (model) into an accessible and yet reliable archive for the future.

LITERATURE REVIEW

Photogrammetry definition by Linder (2009), is measurement using light, mostly using photographs that have all the spectrum characteristics that define depth, distance and sizes that can be analysed into readable measurement and data. In short, photogrammetry is the science of measuring the world using images that are enough and can be calculated to create a 3 Dimensional data for digital usage for the third party. The accuracy of the measurements depends on the technology used, calculation methods and the availability of images that gives the information about the subject into a 3D space and realm.

Photogrammetry is widely used in many fields such as architecture, land surveying, industry and others that require measurements based on the real life structure or objects. It has been improved since the advancement of both hardware and software in the 21st century. It is important to understand as well that photogrammetry uses methods of mathematical measurement and calculations to create a database that is reliable and accurate. Lack of image accuracy such as distorted images or damaged images will affect the accuracy and readability of the measurements (Wolf, Dewitt & Wilkinson, 2014).

Application of photogrammetry in small scaled models can be improved with proper lighting and condition (such as dedicated photo studio) to improve the gradient and colour data accuracy for the software to the analysis to generate a more accurate and reliable 3D modelling for architecture Hallert (2016). Therefore, a proper setup, camera, lighting calibration and background are important in data collection (photoshoot) that can be used by the software to generate a more accurate and detailed 3D model. This can be seen in the proper setting used by a YouTube content creator, Grzegorz Baran (2021) in his testing of 'Photogrammetry Setup for Indoor 3D Prop Scanning' using sculpt model in his small studio setup. This shows the magnificent digitalization in photogrammetry to acquire a very good and acceptable detailing in 3D models for data preservations.



Figure 1.0 Screenshot of Indoor Photogrammetry Test Imagery by Grzegorz Baran (2021).

The same software and technology is used for aerial photogrammetry by surveyors when they need to acquire data for example, real-estate analysis and estimation. Such techniques have been widely used because clients can explore and analyse the land more accurately when using photogrammetry for their estimation input.

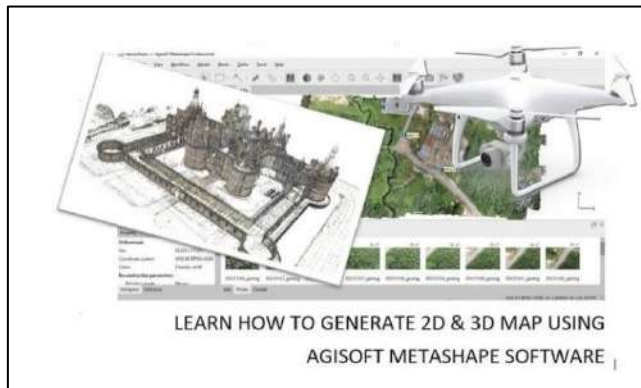


Figure 2.0 Screenshot of Photogrammetry using Drone by Suriyadi Mohamad (Kelab Drone Malaysia) (2021).

METHODOLOGY

A free source software called Agisoft Metashape Professional (64 bit 2020 Version) is used for this experiment and data analysis of images taken in a small studio setup with proper artificial lighting to generate 3D models. Sets of images took using Sony Smartphone Camera that has proper image stabilization and image processing is used to took images (minimum overlaps of 60 to 70%) taken from all angles of the model (front, left, right, top, 360 degrees perspectives) transferred into the personal computer with the software to analyse.

Then, under the workflow tab, the 'align photos' process is done to analyse all the photos taken. This process uses the analysis of colours, shapes and patterns into 'align' settings before the next process takes place. This process sometimes takes about 1 hour to 5 hours to complete depending on the number of images, complexity and processing power of the respective computer.

After that, the process under workflow - 'build mesh' has been done to connect the 3D mesh analysed by aligned photos and a 3D model can be acquired for this. This 3D mesh then can be exported to other software such as sketchup, 3D Max or others that can be used later.

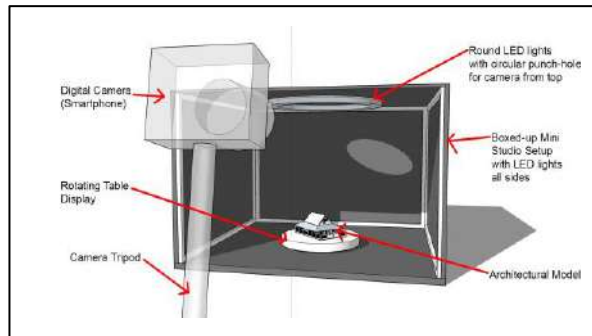


Figure 3.0 Architectural Model Mini Photogrammetry Booth Setup

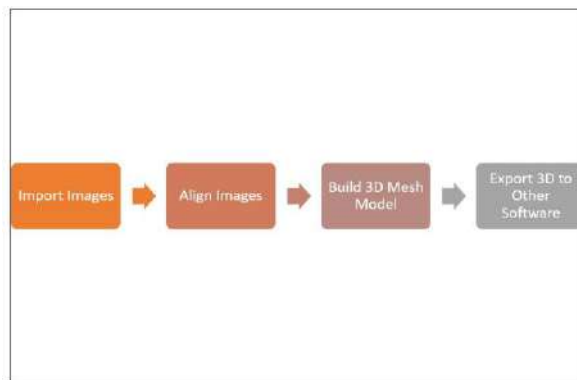


Figure 4.0 Flow of Process to Generate 3D model using Agisoft Metashape Software

FINDINGS

The 3D reproduction of the analysed photographs of the architectural model is 80% to 90% accurate with dimension. The 3D model accuracy and detailing can be improve by below methods:-

- a) improving the image sharpness for every photos taken
- b) number of photos taken (to get most information about the model)
- c) 'depth' area of certain model that has inner details need to be taken photos as well to improve the model details
- d) lighting fixture to enhance (stable and constant lighting)
- e) software Random Access Memories (RAM) and processor (Computer Processing Unit, CPU) to speed up the mesh and images processing for 3D model construction.



Figure 5.0 Equipment used in the 'Mini Studio' setup for photography session

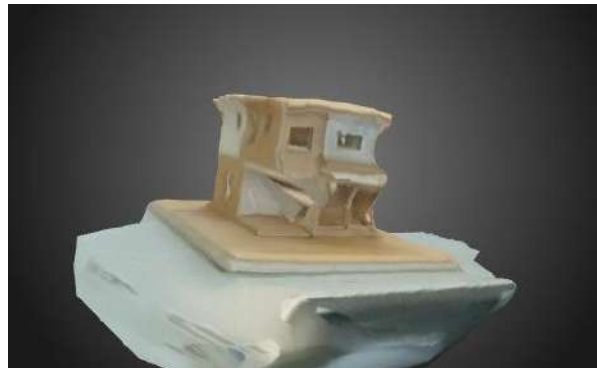


Figure 6.0 3D Images Result from Agisoft Metashape after the experiment (1st Trial)

The above Figure 6.0 shows the 3D mesh and mapping from Agisoft Metashape software after the 1st trial. It shows important data and analysis of 3D models and mapping even though not 100% - it is about 80% and the problem of 'melting images' effects due to the lack of images or triangulation process done.

Better equipment and image processing hardware and software are needed to improve this data collection process to obtain the objectives of the research. This experiment proves that with proper technique and devices, an archive of architectural 3D models can be stored and used for future research and references.

CONCLUSION

As education has evolved and achieved a greater level due to the improvement of both hardware and software, photogrammetry is a science that has a very good potential to produce a good result and achieve the objective of preserving architectural models created by architectural students. Thus, it improves the understanding of photogrammetry and skills of photography among lecturers and students as a whole.

Proper installation of the devices for this project research can enhance the result and all the methods can be used not only in architecture but also other fields such as arts and crafts. The possibility is endless and within proper time given to do more testing and fund, this can be a product that can be used by any other architectural institution to preserve their architectural model not only in a static photo for portfolio but also in a more immersive experience of the model.

It is believed that with this application, it can also be used in Virtual Reality (VR) and Augmented Reality (AR) platforms.

AUTHOR BIOGRAPHY

‘Adil Farizal Md Rashid, PhD is a Faculty Research Head of Faculty of Architecture and Built Environment (FABE), Infrastructure University of Kuala Lumpur. He is one of the recipients of the Gold Award for an innovation project called “Development of Solar Powered Bamboo Catamaran” and the Bronze Award for “Development of Interlocking Industrial Building System for Housing Using Incombustible Plastic Foam” in the Infrastructure University Innovation & Invention Competition (IUIIC 2017). He is a lecturer for both 2 Dimensional (2D) and 3 Dimensional (3D) Computer-Aided Design (CAD) courses for Diploma in Architecture and Bachelor of Science in Architectural Studies for 9 years. His specialty in housing architectural design, design and building construction, and 3D Architectural Visualization has been used for both graphical and presentation works at FABE, IUKL. *Email: adil@iukl.edu.my*

Mr. Rizal Husin is a lecturer and previously an industry player in the field of architecture and the built environment. He is one of the authorized Building Information Modelling (BIM) professionals in the industry. He has been teaching studio and CAD courses for Bachelor of Science of Architecture and holds the position of Head of Program for it. *Email: rizal.husin@iukl.edu.my*

Tuan Haji Md Pilus Md Noor is the Dean, Faculty of Architecture & Built Environment (FABE) for more than 5 years and is highly experienced in the architecture and built environment industry from local authorities to the small architecture firm business. He is a member of education advisory committee for Malaysian Architecture Association since 2011 and is actively involved in education and management in IUKL.

REFERENCES

- A Lake, C Marshall, M Harris, M Blackstein, (2000). Stylized rendering techniques for scalable real-time 3d animation
- Al Asefer M. Marwa & Noor Saadah Zainal Abidin (2021). Soft Skills and Graduates’ Employability in The 21st Century from Employers’ *Perspectives: A Review of Literature*, Vol.9, No. 2, 52(2), 44-59.
- Ali Asad Pour (2021). *Architectural Photogrammetry*. Shiraz University of Arts Architectural Photogrammetry Studio Report
- Cristian Jacquemoin, (2004). Architecture and Experiments in Networked 3D Audio/Graphic Rendering with Virtual Choreographer
- Daniel Tal & John Altschuld (2021). *Photogrammetry. Drone Technology in Architecture, Engineering and Construction*
- David Koller, Michael Turitzin, Mark Levoy, Marco Tarini, Giuseppe Crocchia, Paolo Cignoni, Roberto Scopigno, (2004). *Protected interactive 3D graphics via remote rendering*

- Gerald Weiss, David Vallejo, Luis Jimenex-Linares & Joses Jesus Castro-Schez (2010). A Multiagent Architecture for 3D Rendering Optimization
- K. Khoshelham a, and L. Díaz-Vilariño b (2014). *3D Modelling of Interior Spaces: Learning The Language of Indoor Architecture*
- Konrad Schindler & Wolfgang Forstner (2021). *Photogrammetry. Computer Vision, A Reference Guide*
- S. Cacciaguerra, M. Rocchetti, M. Riffukku, A. Kinu, (2010). A wireless software architecture for fast 3D rendering of agent-based multimedia simulations on portable devices.
- SM Mustapha (2021). The Relationship Between Online Teacher-Student Interaction and Online Academic Performance: *The Mediating Effect of Academic Optimism*, Vol.9, No. 2, 3(4), 1-10.
- SM Mustapha (2014). Students' Classroom Participation: What Drives It?. *International Journal of Research in Education Methodology*, Vol.5, No. 3, 707(2), 699-709.
- Thu Nguyen-Phuoc, Chuan Li, Stephen Balaban, Yong-Liang Yang, (2018). RenderNet: A deep convolutional network for differentiable rendering from 3D shapes
- Yuxuan Zhang, Wenzheng Chen, Huan Ling, Jun Gao, Yinan Zhang, Antonio Torralba, Sanja Fidler, (2021). *Image GANs meet Differentiable Rendering for Inverse Graphics and Interpretable 3D Neural Rendering*

ZERO TRUST SECURITY IMPLEMENTATION CONSIDERATIONS IN DECENTRALISED NETWORK RESOURCES FOR INSTITUTIONS OF HIGHER LEARNING

Atiff Abdalla Mahmoud Arabi, Tadiwa Elisha Nyamasvisva and Sangeetha Valloo
Infrastructure University Kuala Lumpur, Malaysia

ABSTRACT

Unlike conventional perimeter-based security, Zero Trust allows Institutions of Higher Learning (IHL) and related businesses to operate while also modifying security architecture to suit new user demographics, customer interaction models, cloud usage, and IoT devices. The COVID-19 epidemic has prompted widespread transformation, necessitating a quick shift to Zero Trust. Starting with identity and device security, IHLs and related businesses may reduce risk quickly by concentrating on identity management and device security. These two key elements of the Zero Trust ecosystem provide assurance and the institutes will immediately see security advantages from its Zero Trust programme. Implementing Zero Trust is a slow process, as large-scale projects are unlikely to succeed. Working with current security capabilities and progressively moving to a Zero Trust paradigm while implementing important, strategic changes over a set period of time is the core concept of Zero trust Implementation. This paper recommends practices for implementing the five core pillars of Zero Trust in IHLs and related businesses. The pillars discussed are people, workloads, devices, networks, and data.

Keywords:

Network segmentation (MFA), Multifactor authentication, workloads, software-defined networking (SDN), Zero Trust, Parameterised Networks

INTRODUCTION

Zero Trust is quickly becoming the preferred security strategy for both businesses and governments (Deshpande, 2021; Egerton et al., 2021; Mohammed, 2012). As an implementation domain, institutions of higher learning (IHL) are not exempt. However, security professionals in IHL and other application areas are often unsure where to start with Zero Trust implementation or are intimidated by the fundamental changes in strategy and design that Zero Trust necessitates (Jewell et al., 2022; von Faber, n.d.). However, implementing Zero Trust does not need removing all of your existing security measures and starting over, and with the correct methodology, you can start reaping the advantages right now. This study is for security executives who want to learn about the practical components of a successful Zero Trust implementation path (Atiff et al., 2021; Buck et al., 2021; D'Silva & Ambawade, 2021; Xiaojian et al., 2021).

PREREQUISITES FOR IMPLEMENTING ZERO TRUST IN INSTITUTIONS OF HIGHER LEARNING

Zero Trust is a conceptual and architectural framework for transitioning security from a network-oriented, perimeter-based security paradigm to one based on continuous verification of trust (Lowdermilk & Sethumadhavan, 2021). It is based on the original Zero Trust idea. While this may appear to be a straightforward task, it necessitates a mental shift as well as significant adjustments in the implementation and usage of security solutions. It is vital to create a thorough roadmap that specifies the primary workstreams and projects required to accomplish your Zero Trust approach.

Administrators can see the exact delivery schedule, how much money they'll need to invest, and what particular business and security benefits they will get from their investment in Zero Trust. Institutions should review the plan before formalisation:

- i. Set their overall Zero Trust strategy.
- ii. Define the seven core pillars, or components, of Zero Trust in the context of the institute.
- iii. Detail the core institutional capabilities necessary to deliver all the requirements
- iv. Recruit both Institute and IT stakeholders in the development of the roadmap
- v. Identify interdependencies with other security, IT, and Institute projects

The data security component requires that the institute can inventory, classify, archive, or delete data according to policy (Garbis & Chapman, 2021b; Horne & Nair, 2021). Today, no single vendor or provider can deliver all the capabilities and components of zero trust, it will be necessary to partner with multiple providers. Building a practical and pragmatic roadmap will allow the institutes to identify and evaluate the appropriate providers and individual technologies. Recruiting both institute (business) and IT stakeholders in the development of the roadmap the Zero Trust implementation will require new investment or, at a minimum, shifting of investment, and it will also create an avalanche of technical and organizational change. Identifying the key players that are critical for the institute's Zero Trust strategy requires that the institution need to include at a minimum (Garbis & Chapman, 2021a; Lowdermilk & Sethumadhavan, 2021):

- i. The institute's board members (who are often the ultimate decision-makers) and business and IT executives (who will grant you the budget).
- ii. The institute's enterprise architects and application owners (who will ensure Zero Trust supports the broader IT strategy and other projects).
- iii. The institute's IT operations team (who will manage the infrastructure that you are building). They must understand the concerns of each stakeholder and address them.

The institutions need to clarify their vision, listen to the feedback, and communicate in a manner that each stakeholder can comprehend. The institutions need to identify interdependencies with other security, IT, and business projects. A Zero Trust effort needs to include existing security, IT, and business projects (Greenwood, 2021; Wylde, 2021). Projects, including cloud migrations to engaging new business partners, can be the catalysts for Zero Trust transformation. As other stakeholders and participants are recruited, integrate the associated roadmaps into the Zero Trust effort. Institutions need to ensure that they properly map and clearly communicate project dependencies (DUO - CISCO, 2019; Haber, 2020; Horne & Nair, 2021). Care must be taken to consider existing requirements in the plan for example, micro segmentation that is too granular could disrupt existing network functions and hamper the overall schedule of IT operations (Sheikh et al., 2021).

Identifying the Starting Point for Institutions of Higher Learning Zero Trust Implementation

Understanding the institutes current maturity level and where the institute want to be in each period will help focus projects and initiatives. For instance, if an institute has a mature identity and access management capability and have already implemented many of the necessary technologies from multifactor authentication to privileged identity management, they may wish to start with an area such as cloud workload security that is less mature. To begin creating an institute detailed roadmap the following needs to be considered (DUO - CISCO, 2019; Lowdermilk & Sethumadhavan, 2021; Luchenko et al., 2021; Simpson & Foltz, 2021; Teerakanok et al., 2021b).

- i. assessing the maturity of the institute current Zero Trust state
- ii. understanding current business initiatives and security projects for the institute
- iii. documenting where the institute can reuse existing capabilities
- iv. setting goals for the institute's future maturity state and period to achieve it

Establish your current baseline by assessing your Institution of Higher Learning current Zero Trust maturity and establish a baseline of capabilities. Identify current business initiatives and existing

security capabilities. Before starting a Zero Trust initiative, learn what other business initiatives are implementing. Security leaders should take advantage of these changes that the business has already sanctioned to deliver Zero Trust more effectively in their organization. Institutes of Higher Learning must set their desired maturity state and time frames to achieve them.

ROADMAP CONSIDERATION FOR ZERO TRUST IMPLEMENTATION IN INSTITUTES OF HIGHER LEARNING

To compliment the prerequisites for implementing zero trust in institutions of higher learning and the starting point recommendations put forward in the earlier sections, this paper outlines the roadmap considerations for implementing zero trust. In doing so the paper focuses on people, workloads, devices, networks, and data as the main pillars to be considered by the Institutions of Higher Learning before, during, and after adopting zero trust.

Zero Trust Roadmap Considerations for People

Institutes of Higher Learning, anywhere around the world, require platforms that are secure but also intuitive enough to adopt without hurting students experience or staff/faculty experience (Abu-Asba et al., n.d.; Hasan et al., 2018). With students, employees, business partners, and network access equipment all using unique identities with differing access privileges, identity and access management requirements have grown increasingly complex (Ahmed et al., 2020; DelBene et al., 2019). Zero trust for people, as a component of a framework that focuses heavily on identity and access management, is often one of the least mature areas, and one of the top three vectors for external attacks. And being the least mature, it is often the easiest to quickly improve with some essential capabilities and supporting technologies. As the institutes of higher learning develop their roadmap for people as a pillar, the following should be considered. See table 1.

Table 1: IHL Zero Trust Considerations and Justifications for People

No	Consideration	Justification
1	Investment in identity and access management technologies that solve the most critical problems (DelBene et al., 2019)	<ul style="list-style-type: none"> – To justify the monetary costs and potential disruption caused by adopting Zero Trust IAM (Identity and Access Management), security professionals must show how these modern technologies solve the organization’s most pressing people and access problems. – When developing IAM improvements as an expansion of an institute’s larger digital evolution, the chances of project approval, funding, and completion skyrocket. – When implementing multifactor authentication (MFA) and single sign-on (SSO), the implementation helps fix other issues related to compliance, security, and productivity.
2	Application of least privilege (DelBene et al., 2019; Haber, 2020)	<ul style="list-style-type: none"> – Do not provide more access to data and apps than users need. This is one of the most important principles of solid zero trust identity and access management practices. – Institutes of higher learning need an annual proof/access review process whereby managers and applications and data owners review user entitlements and grant or revoke them in an identity management and governance platform.

		<ul style="list-style-type: none"> – Institutes of higher learning must ensure that privileged users do not have access to admin functions on systems they do not need to do their job. – As users move from job to job and project to project, institutes must be sure to retire their access to assets. – Overprivileged users, employees, contingent workers, business partners, and customers and dated access credentials lead to breaches.
3	Retire the password. (Mehraj & Banday, 2020)	<ul style="list-style-type: none"> – While deep-rooted in applications, passwords are snoopable, crackable, and stuffable, representing a significant weakness. – Ensure, at a minimum, that MFA protects critical applications and data assets. Using passwordless authentication methods such as biometrics, tokens, or keys, reduces the surface of man-in-the-middle attacks. – Vendors such as Google, Ivanti, Microsoft, Okta, Secret Double Octopus, Yubico, and others deliver solutions to help kill the password

Zero Trust Roadmap Considerations for Workloads

Upon initiating IHL’s Identification and authentication management projects and initiatives, the IHL need to determine the next Zero Trust pillar on which to focus. The maturity model completed in phase one will help IHLs choose their next Zero Trust initiative. For many institutes of higher learning, devices or workloads will be the next initiative. “The rapid adoption of cloud and the new models of computing that support rapid application development have made workload security an urgent area to mature.”(Ahmed et al., 2020). Table 2 below outlines the consideration for workloads for IHLs.

Table 2: IHL Zero Trust Considerations and Justifications for Workloads

No	Consideration	Justification
1	Robust cloud governance process and structure (Ali et al., 2021; DelBene et al., 2019)	<ul style="list-style-type: none"> – To ensure that governance is an ongoing benefit to security, build a repeatable process not a one-time checkbox compliance exercise. – To ensure proper coverage and scope, as your organization may have many different areas and infrastructure components that it wishes to cover, including on-premises, private, and public clouds, and – To ensure executive support. Cloud governance should also cover cost optimization, budgets, regulatory compliance, and threat detection
2	Inventory and monitor workload configurations (DelBene et al., 2019)	<ul style="list-style-type: none"> – Because of the ease of creation, cloud workloads proliferate very quickly, often without any oversight or formal governance of cloud platform credentials, configuration settings, and even instance creation. – Manual processes or IaaS-specific tools will not cut it institutes of higher learning need a true cross-cloud workload security solution.

		<ul style="list-style-type: none"> - Vendors like CloudPassage, Qualys, and Trend Micro can help
3	Cloud-native security and management solutions (DelBene et al., 2019; Mehraj & Banday, 2020)	<ul style="list-style-type: none"> - Cloud washing and dumb lift and-shift of data and workloads to the cloud without a proper governance structure and oversight lead to data sprawl, inadequate data protection, prohibitive costs, and audit findings. - The configurations and protection appropriate for an on-premises workload are rarely appropriate in a public cloud. - Cloud migrations are a terrific opportunity to re platform, reconfigure, or refactor applications to use cloud-native storage, databases, containerization, and logging

Zero Trust Roadmap Considerations for Devices

To fully adopt a ZT (Zero Trust) framework, institutes of higher learning must be able to monitor, isolate, secure, control, and remove every device that is connected to the network at any given moment (Atiff et al., 2021; Sibghatullah et al., 2021). Most security teams still find securing laptops and mobile devices to be a challenge (Teerakanok, Uehara, & Inomata, 2021). IoT devices will make it exponentially more difficult. In the past few years, numerous compromises against a wide range of connected devices have emerged (Kimani et al., 2019). These threats rely on a range of known and unknown vulnerabilities ranging from botnets to insecure software, weak or non-existent encryption, default plain-text passwords, and insecure communication protocols. Security professionals must create a flexible architecture that can adapt to the evolving threat landscape quickly and effectively. As the development an IHL roadmap gathers momentum, the following should be considered for all kinds of devices as in table 3.

Table 3: IHL Zero Trust Considerations and Justifications for Devices

No	Consideration	Justification
1	Apply network segmentation to manage devices. (Kimani et al., 2019; Sheikh et al., 2021)	<ul style="list-style-type: none"> - IoT network segmentation solutions take an existing network of IoT devices and create zones or micro perimeters to help isolate IoT devices from other IT devices or networks, including the ability to quarantine potentially infected or compromised devices from propagating malware. - Segmenting user and device traffic away from the rest of the network can significantly reduce the risk of cybersecurity incidents.
2	Harden IoT devices. (Kimani et al., 2019)	<ul style="list-style-type: none"> - IoT device hardening solutions enable IoT devices and data integrity through capabilities such as secure firmware, trusted execution environments obscuring, or binary modification to help minimize the risk of device/data tampering and unauthorized access and use of the IoT device and its data. - Device hardening can support secure communications, signed software delivery, and secure patches and application updates.

		<ul style="list-style-type: none"> - Allows for device-based lockdown and application sandboxing. - Vendors in this space include Cisco, Infineon, Intel, and Thales.
3	Reduce user risk created by BYOD (Bring Your Own Device) policies. (Morolong et al., 2020; Stafford, 2020)	<ul style="list-style-type: none"> - BYOD and the increasingly mobile workforce have eliminated the control IT used to have over endpoints that connect to enterprise networks and access data. - Must minimize issues by negating the obviously plain threats that endpoints present such as malicious software infections, ransomware events, and malware. - Must conduct health checks on endpoints before allowing them (eg backdoor and virus programs and software updates especially those related to security) to connect to the network or access systems. - Allow to shut down all the non-used and threat-riddled apps your users want to run on their BYOD devices. - Act prescriptively to gain some control by using software-defined networking (SDN) solutions that push the focus of your enterprise security out to the endpoint. - It may not be “your” endpoint, but it is your network, and you can enforce your security policies on those endpoints if you do it right.

Zero Trust Roadmap Considerations for Networks

The perimeter does not disappear, as it remains. But the perception of the network perimeter has evolved. The perimeter is now “the edge” of your network, whereby users touch or connect to the enterprise. Consider a core principle of Zero Trust by redrawing logical segmentation boundaries around network assets and increasing isolation between segmentations. Authorize and log all access at segmentation boundaries and inspect and log all activity within each network segmentation (Sheikh et al., 2021). The following should be considered as you develop your roadmap:

Table 4: IHL Zero Trust Considerations and Justifications for Networks

No	Consideration	Justification
1	Redraw the boundaries. Draw boundaries to protect resources, not networks. (Rose et al., 2020)	<ul style="list-style-type: none"> - Segment around an application and its associated hosts, peers, and services. - The segmentation policy defines the access that each group has with another group. - The baseline, if generated by sensors, will often include the suggested segmentation policy. - Review it for anomalies before enforcement, of which enforcement of the segmentation policy can be done at each host (via an agent) or via virtual network routing. - Host-based agents are the most common, but some users shy away from them for fear of having to deploy those agents on tens of thousands of endpoints.

		<ul style="list-style-type: none"> – In fully virtualized environments like VMware, use a hypervisor component to enforce the policy.
2	Push controls to the “edge” of the enterprise. (Chen et al., 2020; Guide et al., n.d.)	<ul style="list-style-type: none"> – There are multiple approaches to leveraging the existing north-south perimeter as an inspection zone for all human-generated traffic. – Web gateways operating in explicit-proxy and transparent modes can detect and block risky clicks and stop malware. – Use DNS-based solutions to achieve most of the border security goals while being incredibly simple to deploy.
3	Use modern enterprise firewalls to augment cloud security controls. (Mehraj & Banday, 2020)	<ul style="list-style-type: none"> – The next-generation firewall (NGFW) was the backbone for Zero Trust, and it is even better today. – Today, NGFW are stuffed with crypto chips to decrypt and inspect all traffic transiting a boundary, but virtualized use cases are finally becoming common, too. – Insert a layer of autoscaling virtualized firewalls or IDS/IPS behind a gateway load balancer to inspect your application traffic. – Integrate the management of container security policies and cloud firewalls into their cloud-delivered or cloud-connected security dashboards, signalling a path forward where third parties manage cloud objects on your behalf.

Zero Trust Roadmap Considerations for Data

ZT is a much more data- and identity-centric approach to security than a network-focused one or rather the historical approach. This involves building capabilities for visibility into the interaction between users, apps, and data across a multitude of devices and the ability to set and enforce one set of policies irrespective of whether the user is connected to the corporate network. This is not easy and is compounded by the challenge of understanding what is sensitive and valuable data for the organization today. Typically, basic data security controls are already established due to compliance requirements (Ahmed et al., 2020; Mehraj & Banday, 2020); Institutions of higher learning feel they have stopped the bleeding, buying themselves a bit more time yet everything is premeditated by the perpetrators (Nyamasvisva et al., 2020)(Elisha Tadiwa Nyamasvisva, Atiff Abdalla Mahmoud Arabi, Abudhahir Buhari, Fares Anwar Hasan, 2020). However, there is need to evaluate all the Zero Trust pillars together in the context of your critical applications, data, and assets. While building your roadmap:

Table 5: IHL Zero Trust Considerations and Justifications for Data

No	Consideration	Justification
1	Define your data to understand what you must protect, where, and how. (Ahmed et al., 2020)	This includes building capabilities for data discovery and classification to help identify where data is located, and what is sensitive data. These capabilities are readily available today as a feature of other technology offerings as well as from specialized offerings. Work with the risk and privacy Institutions of higher learning to help define the policies around this.
2	Dissect your data to understand its value and lifecycle, and threats to it. (Embrey, 2020)	This data intelligence provides business and contextual insights about data to help guide policies and controls. It requires processes and technologies to help answer questions about your data, such as: <ul style="list-style-type: none"> • How does this data flow to produce a business outcome? • Who is using this data, how often, and for what purpose? • Why does the business have this data, how is it collected, and what is its useful lifecycle? • What are the consequences if data integrity is compromised? In addition, understand the threats to the data collected from other security tools in your environment, such as DLP and EDR, to help guide decision-making.
3	Defend your data through four core measures and enabling technologies. (Assunção, 2019; Shore et al., 2021)	These include controlling access, inspecting data usage patterns, defensible disposal of data, and obfuscation. There are many key technologies to support data security and privacy. Encryption alone encompasses a variety of separate offerings from email encryption to database encryption, to support protecting data in its various states (at rest, in transit, and in use), as well as innovations like homomorphic encryption and quantum-safe offerings

RECOMMENDATIONS

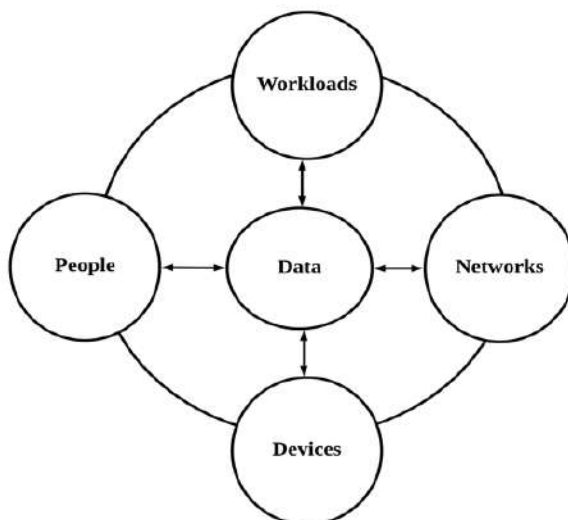


Figure 1: The Recommended Mapping of Zero Trust for Institutions of Higher Learning (IHLs)

The thesis of this paper is summarised in the diagram above which shows the relationships between the pillars of Zero trust.

Bring your ZT (Zero Trust) strategy and roadmap right to the institutions board (DelBene et al., 2019). Chief Information Security Officers (CISOs) have become common fixtures in boardrooms, communicating complex issues and engaging board members' hearts and minds on the topic of security (DUO - CISCO, 2019). This is shifting the boards from having a vague awareness that security threats are real to having an actual understanding of what these threats are and how to tackle them. They are asking tough questions that increasingly demonstrate they understand that the old way of doing security is no longer sufficient. Courageous CISOs are taking Zero Trust to the boardroom (DUO - CISCO, 2019).

To be successful the organization must be clear that ZT is what will get you customer trust. To some, the concept of Zero Trust seems at odds with engendering trust. Build engaging ZT content to meet your board's expectations. The security team must manage cybersecurity like any other risk. Translate technology needs to business benefits. Do not focus on validating more technology just to acquire more technology. The goal of security is to make business better and better to protect your customers' data. Not having more cool security tools. If done right, there should be culling of technologies that do not align with business needs and removing solutions that are not optimal for your strategy.

AUTHOR BIOGRAPHY

Atiff Abdalla Mahmoud Arabi is student of the postgraduate programme PhD (Information Technology) at Infrastructure University Kuala Lumpur (IUKL) Faculty of Engineering, Science and Technology. He obtained his BIT and Masters in IT in Networking from IUKL. His research interests include Zero Trust, Biometrics Authentication, and Prevention of Network-Based Academic Dishonesty. *Email: atiff2009@gmail.com*

Tadiwa Elisha Nyamasvisva, PhD is a member at the Faculty of Engineering and Science Technology in IUKL. His research interests are in Computer Algorithm Development, Data Analysis, Networking and Network Security, and IT in Education. *Email: tadiwa.elisha@iukl.edu.my*

Sangeetha Valloo, is a faculty member at the Faculty of Engineering and Science Technology in IUKL. Her research interests are in Data Communication and Networking as well as Network Security. She was a former Dean at the Faculty of Creative Media and Information Technology in IUKL. Currently, she manages and coordinates all final year projects for the Department of Information Technology at the Faculty. *Email: sangeetha@iukl.edu.my*

REFERENCES

- Abu-Asba, A., Azman, H., Mustaffa, R., & Ali, F. (n.d.). TEACHING STYLES OF YEMENI SCIENCE TEACHERS. *RESEARCH JOURNAL (IUKLRJ)*, 53.
- Ahmed, I., Nahar, T., Urmi, S. S., & Taher, K. A. (2020). Protection of sensitive data in zero trust model. *Proceedings of the International Conference on Computing Advancements*, 1–5.
- Ali, B., Gregory, M. A., & Li, S. (2021). Uplifting Healthcare Cyber Resilience with a Multi-access Edge Computing Zero-Trust Security Model. *2021 31st International Telecommunication Networks and Applications Conference (ITNAC)*, 192–197.
- Assunção, P. (2019). A zero trust approach to network security. *Proceedings of the Digital Privacy and Security Conference 2019*.
- Atiff, A., David, A., & Elisha, T. (2021). A Zero-Trust Model-Based Framework For Managing Of Academic Dishonesty In Institutes Of Higher Learning. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(6), 5381–5389.
- Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, 110, 102436.
- Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., & Zhai, Y. (2020). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, 8(13), 10248–10263.
- D’Silva, D., & Ambawade, D. D. (2021). Building a zero trust architecture using Kubernetes. *2021 6th International Conference for Convergence in Technology (I2CT)*, 1–8.
- DelBene, K., Medin, M., & Murray, R. (2019). The Road to Zero Trust (Security). *DIB Zero Trust White Paper*, 9.
- Deshpande, A. (2021). A Study on Rapid Adoption of Zero Trust Network Architectures by Global Organizations Due to COVID-19 Pandemic. *New Visions in Science and Technology Vol. 1*, 26–33.
- DUO - CISCO. (2019). *Zero Trust Evaluation Guide For the Workforce*. 29.
- Egerton, H., Hammoudeh, M., Unal, D., & Adebisi, B. (2021). Applying Zero Trust Security Principles to Defence Mechanisms Against Data Exfiltration Attacks. *Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications*, 57–89.
- Elisha Tadiwa Nyamasvisva, Atiff Abdalla Mahmoud Arabi, Abudhahir Buhari, Fares Anwar Hasan, J. R. (2020). Prevalence of Premeditated Academic Dishonesty at University Level. A Case Study. *Journal of Critical Reviews*, 7(15), 4494–4501. <http://search.ebscohost.com/login.aspx?direct=true&db=ehh&AN=144463015&lang=es&site=ehost-live>
- Embrey, B. (2020). The top three factors driving zero trust adoption. *Computer Fraud & Security*, 2020(9), 13–15.
- Garbis, J., & Chapman, J. (2021a). *Zero Trust Security: An Enterprise Guide*.

- <https://doi.org/10.1007/978-1-4842-6702-8>
- Garbis, J., & Chapman, J. (2021b). *A Zero Trust Policy Model* (pp. 211–238).
https://doi.org/10.1007/978-1-4842-6702-8_17
- Greenwood, D. (2021). Applying the principles of zero-trust architecture to protect sensitive and critical data. *Network Security*, 2021(6), 7–9.
- Guide, A. E., Garbis, J., & Chapman, J. W. (n.d.). *Zero Trust Security*.
- Haber, M. (2020). *Zero Trust* (pp. 295–304). https://doi.org/10.1007/978-1-4842-5914-6_22
- Hasan, M. M., Ibrahim, F., Mustapha, S. M., Islam, M. M., & Al Younus, M. A. (2018). The use of YouTube videos in learning English language skills at tertiary level in Bangladesh. *IUKL Res. J*, 6, 27–36.
- Horne, D., & Nair, S. (2021). *Introducing Zero Trust by Design: Principles and Practice Beyond the Zero Trust Hype*. April.
- Jewell, D. O., Jewell, S. F., & Kaufman, B. E. (2022). Designing and implementing high-performance work systems: Insights from consulting practice for academic researchers. *Human Resource Management Review*, 32(1), 100749.
- Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, 25, 36–49.
- Lowdermilk, J., & Sethumadhavan, S. (2021). *Towards Zero Trust: An Experience Report*. <https://doi.org/10.1109/SecDev51306.2021.00027>
- Luchenko, Y., Semenova, V., & Kravets, N. (2021). Zero Trust Technology Application for Ai Medical Research. *Грааль Науки*, 10, 264–267. <https://doi.org/10.36074/grail-of-science.19.11.2021.049>
- Mehraj, S., & Banday, M. T. (2020). Establishing a Zero Trust Strategy in Cloud Computing Environment. *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 1–6. <https://doi.org/10.1109/ICCCI48352.2020.9104214>
- Mohammed, I. A. (2012). Analysis of Identity and Access Management alternatives for a multinational information-sharing environment. *INTERNATIONAL JOURNAL OF ADVANCED AND INNOVATIVE RESEARCH*, 1(8), 1–7.
- Morolong, M. P., Shava, F. B., & Gamundani, A. M. (2020). Bring Your Own Device (BYOD) Information Security Risks: Case of Lesotho. *International Conference on Cyber Warfare and Security*, 346–XVI.
- Nyamasvisva, E. T., Arabi, A. A. M., Buhari, A., Wong, F., & Valloo, S. (2020). Premeditated Academic Dishonesty: An IoT Based Preventive Solution. *Solid State Technology*, 63(6), 19369–19379.
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (2nd Draft)*. National Institute of Standards and Technology.
- Sheikh, N., Pawar, M., & Lawrence, V. (2021). *Zero trust using Network Micro Segmentation*. <https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645>
- Shore, M., Zeadally, S., & Keshariya, A. (2021). Zero Trust: The What, How, Why, and When. *Computer*, 54(11), 26–35.
- Sibghatullah, H. M. S., Nyamasvisva, T. E., Arabi, A. A. M., & Buhari, A. (2021). An Ad Hoc Movement Monitoring Algorithm for Indoor Tracking During Examinations. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(3), 3840–3846. <https://doi.org/10.17762/turcomat.v12i3.1672>
- Simpson, W. R., & Foltz, K. E. (2021). Maintaining zero trust with federation. *International Journal of Emerging Technology and Advanced Engineering*, 11(5), 17–32. https://doi.org/10.46338/IJETAE0521_03
- Stafford, V. A. (2020). Zero trust architecture. *NIST Special Publication*, 800, 207.
- Teerakanok, S., Uehara, T., & Inomata, A. (2021a). Migrating to zero trust architecture: reviews and challenges. *Security and Communication Networks*, 2021.

- Teerakanok, S., Uehara, T., & Inomata, A. (2021b). Migrating to Zero Trust Architecture: Reviews and Challenges. *Security and Communication Networks*, 2021. <https://doi.org/10.1155/2021/9947347>
- Von Faber, E. (n.d.). *On the future of IT security management in the face of changes in technology and service delivery*.
- Wylde, A. (2021). Zero trust: Never trust, always verify. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2021*. <https://doi.org/10.1109/CyberSA52016.2021.9478244>
- Xiaojian, Z., Liandong, C., Jie, F., Xiangqun, W., & Qi, W. (2021). Power IoT security protection architecture based on zero trust framework. *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, 166–170.

Finite Element Analysis on the Steel Fiber-Reinforced Concrete Beams: A Systematic Review

Hou Zhicheng & Norhaiza Nordin

Sqlia Types and Techniques - A Systematic Analysis of Effective Performance Metrics for SQL Injection Vulnerability Mitigation Techniques

Aduragbemi David Ogundijo, Atiff Abdalla Mahmoud Arabi & Tadiwa Elisha Nyamasvisva

Technology Acceptance in Tourism Sector: A Systematic Review

Sulaiman Al Jahwari, Mohd. Dan Bin Jantan & Supriya Pulparambil

A Comprehensive SWOT Analysis for Zero Trust Network Security Model

Tadiwa Elisha Nyamasvisva & Atiff Abdalla Mahmoud Arabi

Women Leadership in Malaysian Creative Industry

Kartini Kamalul Ariffin & Faridah Ibrahim

Preservation of Architectural Model into 3 Dimensional Digital Form with the Methods of Photogrammetry

Adil Farizal Md Rashid, Rizal Husin & Md Pilus Md Noor

Zero Trust Security Implementation Considerations in Decentralised Network Resources for Institutions of Higher Learning

Atiff Abdalla Mahmoud Arabi ,Tadiwa Elisha Nyamasvisva & Sangeetha Valloo