SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

An Active Cyber Insurance Policy Against Cybersecurity Risks Using Fuzzy Q-Learning

Ahmad Kamal Ramli[1,*]

[1] Computing Sciences Studies, College of Computing, Informatics and Media, Universiti Teknologi MARA(UiTM) Pahang Branch, Raub Campus, 27600 Raub, Pahang, Malaysia

ARTICLE INFO

Article history:
Received 23 February 2023
Received in revised form 30 April 2023
Accepted 1 May 2023
Available online 15 May 2023

Keywords:
Cyber Insurance; Cyber Risks; Cybersecurity; Fuzzy; Reinforcement Learning; Autonomous Computing

ABSTRACT

Insurance is an extremely diversified from one clear-cut policy to another depending on a rising demand. Internet based businesses are a booming industry and falls under categories of small, medium and enterprise. It is no exception that cybersecurity risks are exponentially presents as a continues fears in this business environment. To ensure this insecurity is handled effectively, cyber insurance policies introduced by insurance companies. However, the nature of cyber risks must be addressed in much more robust and complex algorithms. Autonomic computing with the combination of Fuzzy and Q-Learning is introduced to ensure active policies are ready to handle the uncertainty and together with the ability to learn and mitigate the unrest situation.

1. Introduction

Conventional approaches of insurance are situation-based approaches and amount of pool money collected from the subscribed and active policies. Such as car insurance, medical insurance, fire insurance etc. The amount of fire insurance can be as low as RM 100 per month due to the frequency of losses and damage to a structure damaged in the event of fire, active policies, and pool money present. Similarly with car insurance, insurance companies can predict the exponential amount of those cars and depreciation values from one year to another. According to the survey conducted by Statista [21], about 61 percent of respondents in Malaysia on year 2019 said they possessed a car.

Cyber insurances are more robust and dynamic due to the nature of business that relates to global transactions every second. Companies involved with data transactions that are heavily influenced with cyber risks are actively under constant pressure to get a reliable policy to ensure there is no unwanted situations occurs. The risks are very vigorously presents in many conditions such as legacy software, hardware, malware applications, security, tons of Internet of Things (IoT) devices [26],

[*] *Corresponding author.*
E-mail address: kamalramli@uitm.edu.my

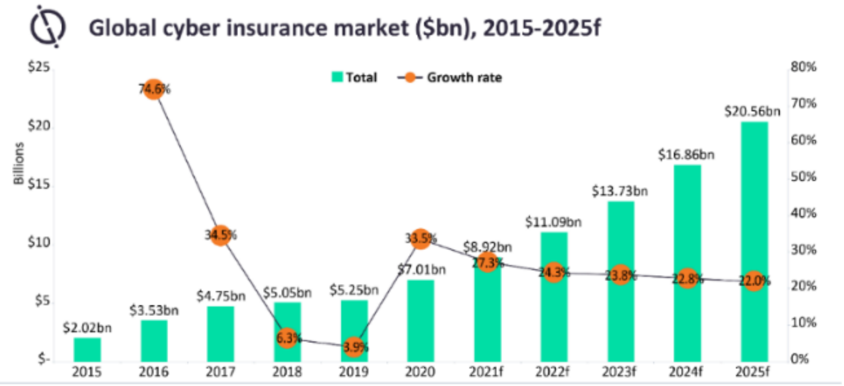
https://doi.org/10.37934/araset.30.3.212221

developments of smart city [27], underutilized of smart technologies in modular transportation [28], assessments and human factors.

There is an inclusive contingency situation, and some are exclusive from the agreed agreement. Global insurance was worth $7bn in gross written premiums in 2020 and expected to be $20.6bn by 2025 [1]. Cyber security is in the highlight due to the Covid-19 pandemic issues that advised businesses to effectively run on internet technologies. This is clearly unrest situations where companies are not ready with the feasibility of working remotely and at the same time lacks a decent application and technologies to ensure ad hoc connections are well managed by security software or technical experts. This is clearly a great opportunity for cybercriminals to strike and make use of pandemic situations. The affected industries are [20].

I. Financial Services
II. Healthcare
III. Education
IV. Energy and Utilities Industries
V. Government Agencies

Malaysian insurance companies such as AIG (American International Group] and MSIG (Mitsui Sumitomo Insurance Group) are actively ready with cyber insurance policies [7,29]. But then, due to the global threats of cyber risks, premium amount paid vary depending on the checked check list in the subscribed policy. Claim protocols is the hire wire modes to cater to the urgencies based on the reported cyber risks. A professional computer expert will be appointed as the adjuster to thoroughly review the incidents and value the possible amount for reimbursement. Figure 1 illustrates the global insurance market in USD Billion from the year 2015-2025.



Source: GlobalData, Insurance Intelligence Center

Fig. 1. Global cyber insurance market 2015-2025 [9]

Thus, this paper introduced the combination of Fuzzy and Q-Learning to handle cyber risks and mapped that with insurance active policies. Several research related to fuzzy rules are presented on other applications and able to handle uncertainty [18,19], whereby Q-Learning is one of the algorithms in Reinforcement Learning with the ability to cater on policy approach [22]. On policy in a nutshell is to ensure there is no misguide and very details in every step adopted and very useful to tackle active policy and global cyber risk. It is a combination of automated framework and works in autonomic computing.

1.1 Literature Review

In insurance, the terms Perils referred to harm, natural causes, and human causes. The translation of that to cyber risks are [14]:

I. Abusive Content
II. Availability
III. Fraud
IV. Information Gathering
V. Information Security
VI. Intrusions
VII. Malicious Code
VIII. Vulnerability

To mitigate the cyber risks, seven prevention risks are as below.

I. Develop Standards
II. Common language and good practices
III. Scenario Analysis
IV. Dialogues with stakeholders
V. Follow-up on technical development
VI. Further develop analytical and modelling skills.
VII. Secure own systems [2]

Crypto mining, ransomware, business email compromises, web application vulnerabilities [25], spear phishing is a new language of business risk [3]. It can be a massive data breach or automated attacks that exploit the classified data to unwanted parties. This leads to cybercrime economy and lots of cyber components introduced by the cyber communities [5]. The inconsistency of blockchain implementation from one country to another, either controlled by central banks or own financial institutions are exposed to cyber threats. This is mainly due to the loose regulations and maturity of the blockchain technology [24].

1.1.1 Cyber insurance scenarios

1.1.1.1 Case 1

Investment advisory firm received routine email request to transfer USD 480.000.00. The email purporting to be their client. After the transfer, it was determined that funds were sent to a cybercriminal. The insured amount is USD 1 million and is subject to a USD 5 000.00 retention. Insurance covers the funds lost [3].

1.1.1.2 Case 2

A patient alleged that nurse accessed her medical records and disclosed that to a third party without her permission. The matter was settled out of court with five-figure settlements covered by the insurance agreement [3]. The common policy among insurance companies will pay for loss are as below [4,6,7].

I. Breach of Personal Information
II. Breach of Corporate Information
III. Contamination of Third-Party Data

The Bayesian Network Model used by [15] can model Conditional Probability based on hazards, peril, and impact from cyber-attacks. Risk level impact based on nine cyber-attacks illustrated in Figure 2.

Risk Level Impact		
Cyber Attacks	TRUE	FALSE
Malicious code	1.03 × 10-11	0
Vulnerability	1.03 × 10-11	0
Abusive content	0.90 × 10-11	0
Information gathering	0.77 × 10-11	0
Intrusions	0.64 × 10-11	0
Fraud	0.13 × 10-11	0
Information Security	0	0
Intrusion attempts	0	0
Availability	0	0

Fig. 2. Risk level impact [15]

Pikkin Lau *et al.* [16], focuses on the cyber risks in power systems deploying smart technologies. A novel mutual insurance model runs on epidemic network model. It measures the transmission grids and substations performance due to cyber-attacks. The model itself can detect effectiveness of mutual insurance in five transmission grids. Risk assessment with threat modelling and threat scoring applied in [17] to identify threat exists in each application process. Elements captured are;

I. Data Collection
II. Decompose Application
III. Threat Identification
IV. Threat Classification using STRIDE
V. Threat measurement using DREAD
VI. Evaluation
VII. Validation

In a fuzzy system, the research made by Kohli *et al.* [18] and Defazio *et al.* [19] demonstrates the benefit of the adaptation of the available services together with Service Level Agreement (SLA). The adaptation can increase profits and deal with the negotiations [20]. An analysis with only Fuzzy approach researched by Alali *et al.* [12] to identify the components of cyber risk, it then supported by MAPE-K approach on separate occasion [13]. Therefore, in this research, the Monitor, Analyze, Plan, Execute and Knowledge Base (MAPE-K) equipped with self-properties, which is the combination of Fuzzy and Q-Learning interacting with the assigned components iteratively within the loops [11].

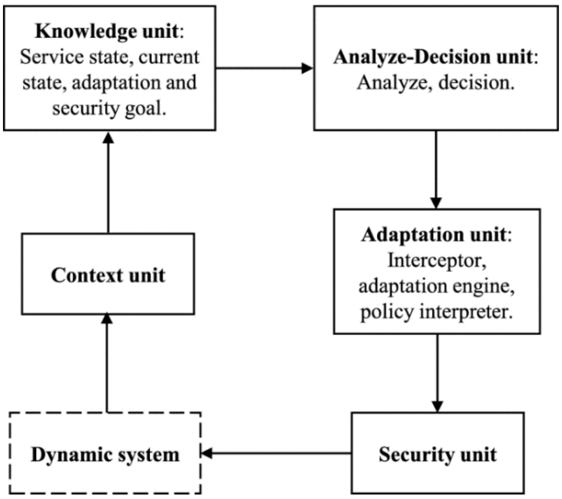

Knowledge unit: Service state, current state, adaptation and security goal.
Analyze-Decision unit: Analyze, decision.
Context unit
Adaptation unit: Interceptor, adaptation engine, policy interpreter.
Dynamic system
Security unit

Fig. 3. Adaptive security based on MAPE-K [11]

2. Proposed Framework

The adaptation framework as below;

I. Autonomic Controller
   i. The whole framework is based on the autonomic computing environment.

II. Knowledge Learning
   i. This element consists of the system state, system goal, and adaptive policy. All these three are connected.

III. Fuzzy Logic Controller
   i. This is the phase where a set of predefined rules on the framework elements is developed and tabulated.

IV. Output.
   i. The output is generated on the successful condition and returns to the current iteration state for another round of loop to iteratively enhance and update framework security elements.

The risk of cyber security fall under the two categories of issues.

I. Qualitative
   Rely on Rating and Relative

II. Quantitative
   Impact-based Matrix

The establishment of fuzzy rules narrowed as very low, low, medium, high, and very high. An example of the simulation using rule base and connection to the relatives illustrates in Table 1 and Table 2. Figure 4 is the Q-Learning framework that integrates with fuzzy rules.

Table 1
Fuzzy Legends

Relative Values	
Very Low	0.5
Low	1
Medium	1.5
High	2
Very High	2.5
Value 1	Cyber Risk A
Value 2	Cyber Risk B
Value 3	Cyber Risk C

Table 2
Rule base Approach

	Rule base Approach			
Rules	Value 1	Value 2	Value 3	Result
1	Low	Low	Low	Very Low
2	Low	Low	Medium	Very Low
3	Low	Low	High	Low
4	Low	Medium	Low	Very Low
5	Low	Medium	Medium	Low
6	Low	Medium	High	Medium
7	Low	High	Low	Low
8	Low	High	Medium	Medium
9	Low	High	High	High
10	Medium	Low	Low	Very Low
11	Medium	Low	Medium	Low
12	Medium	Low	High	Medium
13	Medium	Medium	Low	Low
14	Medium	Medium	Medium	Medium
15	Medium	Medium	High	High
16	Medium	High	Low	Medium
17	Medium	High	Medium	High
18	Medium	High	High	Very High
19	High	Low	Low	Low
20	High	Low	Medium	Medium
21	High	Low	High	High
22	High	Medium	Low	Medium
23	High	Medium	Medium	High
24	High	Medium	High	Very High
25	High	High	Low	High
26	High	High	Medium	Very High
27	High	High	High	Very High

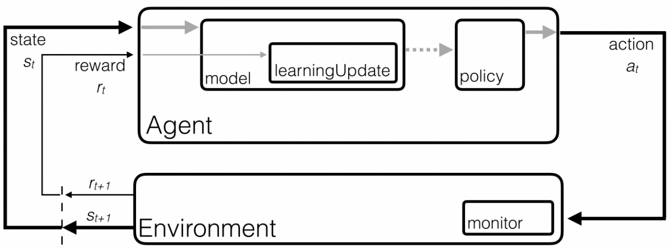


Fig. 4. Q – Learning framework [24]

Implementation of the Complete Algorithm

Phase One.

1. Acceptance of the three Cyber Risk Parameters (Value 1, Value 2 and Value 3).

Phase Two

1. Execution of submitted parameters (Very Low, Low, Medium, High, Very High) to center of weighted approach.
    - Use scores for each performance.
    - Use reward for Q-Learning algorithm.
    - Populate the values for the next phase.

Phase Three

1. Application of fuzzy for membership functions and rule base

Phase Four

i. Comparison of three parameters

Phase Five

1. Analysis of the results.

Since the fuzzy and MAPE-K are connected iteratively, the pre identified rules will undergo few loops to ensure it is adaptive to the new identified risks and enhanced rules. At this stage, the policy is the key to understanding the iterative process and the adaptation.

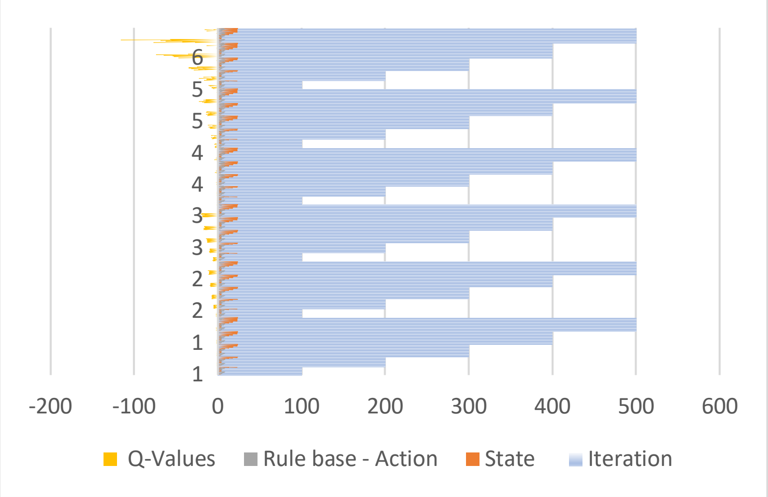


Fig. 5. Cyber Risk A versus Cyber Risk C

Q-values in Figure 5 and Figure 6 explains the adaptation of q-learning parameter with the number of rule base and iteration. State refers to the ability of that parameter to catch up with the highlighted risks.

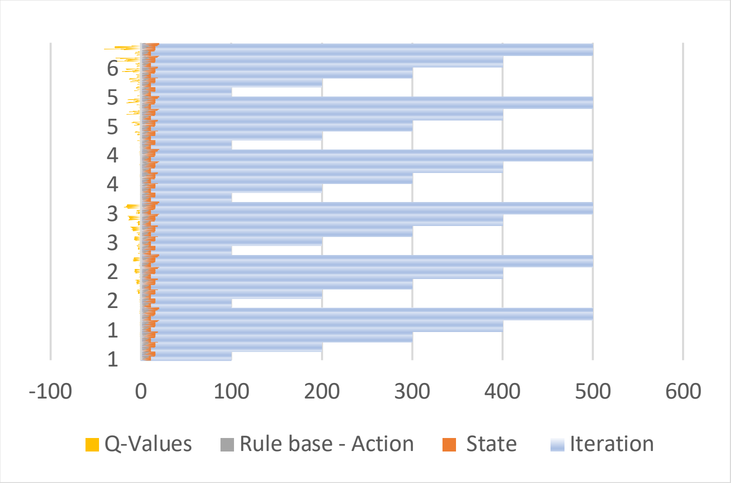


Fig. 6. Cyber Risk B versus Cyber Risk C

Every completed episode is another level of adaption, and it mitigates discovered cyber risks based on robust metrics.

3. Analysis

As stated earlier, the active insurance policies are very much related to the unrest cyber risks incidents happening locally and globally. Every incident does affect active insurance policy whether issued by single insurance companies or collaboratively among them. The latest risk can either be the new or growing risk from the identified harms. Therefore, it will eventually increase the amount of premium related to that particular risk. We understand that insurance policy warrants on the same risks vary from one company to another. Some of them will issues an aggregate limit on the repeatable risk.

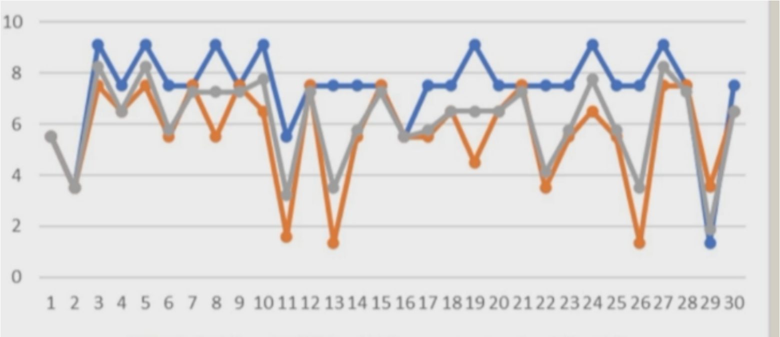


Fig. 7. Comparison of Cyber Risk A, Cyber Risk B and Cyber Risk C

Figure 7 illustrates the comparison of results gathered between the specified risks. This is purely fuzzy rule based 27 rules. Cyber Risk A (blue), Cyber Risk B (grey) and Cyber Risk C (orange). Cyber Risk A mostly dominates the result on every repeatable incident. An example of cyber risk categories:

I. Cyber Risk A = Soft Skills, such as hacking, phishing, password etc
II. Cyber Risk B = Hard Skills, such as face to face communication, social engineering etc

III. Cyber Risk C = Emotional

Cyber Risk C is very less affected, and this is mainly due to the simulation based on corporate subscribers. This result eventually contradicts if it is on personal internet users. In Figure 6, we can see the learning parameters are adapting to that specific rule base. More values of Q-Learning require securing Cyber Risk A, unlike Cyber Risk B and Cyber Risk C. The connection of all cyber risks is important to cyber insurance companies and how that helps the development of policy-based approaches. Simple and straightforward policies are less adaptable with the cyber risks presented currently.

4. Conclusions

Global cyber risks are the daily battle for internet-based companies. This growing pressure with the cloud based, big data, Internet of Things (IoT), autonomic computing etc. Insurance companies are seen as the one stop solution to handle this effectively with a premium amount of money to be allocated to the introduced policy. Adaptive policy-based management is the present and future solution for cyber insurance companies. With the combination of Fuzzy and MAPE-K, it shows the benefits of the proposed framework to ensure both parties really understand the risks they are facing.

The extension of this research is to focus on the full implementation of autonomic computing with autonomic elements. Every element can make their own decision based on active and present assessment of running cyber risks. Such as, in the event of outbreak, policy from insurance company A, able to discuss with company B to handle any excess amounts for incoming cyber risks. The negotiation is based on the aggregate limits authorized to each element. Admission control on the policies from any insurance company and it is integrated with the autonomic computing are highly encourages for future research related to this paper.

Acknowledgement

This research was not funded by any grant.

References

[1] https://www.globaldata.com/cyber-insurance-industry-exceed-20bn-2025-says-globaldata/
[2] https://slidetodoc.com/cyber-risk-and-cyber-insurance-anna-maria-dhulster/
[3] https://www.insurancejournal.com/research/research/2019-cyber-claims-digest/
[4] https://www.chubb.com/my-en/business/cyber-insurance.html
[5] Managing the impact of COVID-19 on cyber security. PwC – White Paper.
[6] https://www.aig.my/business/products/financial-lines/cyber-insurance
[7] https://www.aon.com/apac/cyber-solutions/cyber-insurance
[8] https://www.consultancy.eu/news/4695/number-of-claims-on-cyber-insurance-policies-rising-steeply
[9] https://www.globaldata.com/cyber-insurance-industry-exceed-20bn-2025-says-globaldata/
[10] https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2020.html
[11] Lara, Evangelina, Leocundo Aguilar, Mauricio A. Sanchez, and Jesús A. García. "Adaptive security based on mape-k: A survey." Applied Decision-Making: Applications in Computer Sciences and Engineering (2019): 157-183. https://doi.org/10.1007/978-3-030-17985-4_7
[12] Alali, Mansour, Ahmad Almogren, Mohammad Mehedi Hassan, Iehab AL Rassan, and Md Zakirul Alam Bhuiyan. "Improving risk assessment model of cyber security using fuzzy logic inference system." Computers & Security 74 (2018): 323-339. https://doi.org/10.1016/j.cose.2017.09.011
[13] Elgendi, Ibrahim, Md Farhad Hossain, Abbas Jamalipour, and Kumudu S. Munasinghe. "Protecting cyber physical systems using a learned MAPE-K model." IEEE Access 7 (2019): 90954-90963. https://doi.org/10.1109/ACCESS.2019.2927037

[14] S. Jiwasurat, & C. Mitrpant, The history of Thaicert: from the Ministry of Science and Technology to the Ministry of Digital Economy and Society. [Online]. Available: https://www.thaicert.or.th/papers/general/2012/pa2012ge001.html.

[15] Jeamaon, Aomduan, and Chaiyaporn Khemapatapan. "Cybersecurity Risk Assessment for Insurance in Thailand using Bayesian Network Model." In 2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), pp. 257-260. IEEE, 2022. https://doi.org/10.1109/ECTIDAMTNCON53731.2022.9720387

[16] Lau, Pikkin, Lingfeng Wang, Wei Wei, Zhaoxi Liu, and Chee-Wooi Ten. "A Novel Mutual Insurance Model for Hedging Against Cyber Risks in Power Systems Deploying Smart Technologies." IEEE Transactions on Power Systems 38, no. 1 (2022): 630-642. https://doi.org/10.1109/TPWRS.2022.3164628

[17] Oktorianto, Bintang, Moh A. Amin Soetomo, and Charles Lim. "Risk Assessment For Enterprise Application In The Insurance Sector." In 2021 6th International Conference on New Media Studies (CONMEDIA), pp. 124-128. IEEE, 2021. https://doi.org/10.1109/CONMEDIA53104.2021.9617196

[18] Kohli, Manbeen. "An Enhanced Goal-Oriented Decision-Making Model for Self-Adaptive Systems." (2011).

[19] Defazio, Aaron, and Thore Graepel. "A comparison of learning algorithms on the arcade learning environment." arXiv preprint arXiv:1410.8620 (2014).

[20] https://processbolt.com/top-5-industries-most-vulnerable

[21] https://www.statista.com/statistics/1029277/malaysia-car-ownership-among-consumers/

[22] Shen, Danyating, Takara Truong, and Cortney Weintz. "Using Q-Learning to Personalize Pedagogical Policies for Addition Problems." In 2021 International Conference on Signal Processing and Machine Learning (CONF-SPML), pp. 186-189. IEEE, 2021. https://doi.org/10.1109/CONF-SPML54095.2021.00043

[23] https://blog.twitter.com/engineering/en_us/topics/open-source/2016/reinforcement-learning-for-torch-introducing-torch-twrl.html

[24] Hassan, Mohd Sayuti, Siti Fairuz Mohd Radzi, and Nurul Syuhada Shaari. "Security, Sustainability, and Legal Issues of Blockchain Technology Implementation: A Short Literature Review." Journal of Advanced Research in Applied Sciences and Engineering Technology 30, no. 1 (2023): 275-281. https://doi.org/10.37934/araset.30.1.275281

[25] Ali, Firkhan Ali Hamid, Mohd Khairul Amin Mohd Sukri, Mohd Zalisham Jali, Muhammad Al-Fatih, and Mohd Azhari Mohd Yusof. "Web-Based Reporting Vulnerabilities System for Cyber Security Maintenance." Journal of Advanced Research in Applied Sciences and Engineering Technology 29, no. 3 (2023): 198-205. https://doi.org/10.37934/araset.29.3.198205

[26] Kelian, Virakwan Hai, Mohd Nazri Mohd Warip, R. Badlishah Ahmad, Phaklen Ehkan, Fazrul Faiz Zakaria, and Mohd Zaizu Ilyas. "Toward Adaptive and Scalable Topology in Distributed SDN Controller." Journal of Advanced Research in Applied Sciences and Engineering Technology 30, no. 1 (2023): 115-131. https://doi.org/10.37934/araset.30.1.115131

[27] Shwedeh, Fanar, Norsiah Hami, Siti Zakiah Abu Bakar, Fadhilah Mat Yamin, and Azyyati Anuar. "The Relationship between Technology Readiness and Smart City Performance in Dubai." Journal of Advanced Research in Applied Sciences and Engineering Technology 29, no. 1 (2022): 1-12. https://doi.org/10.37934/araset.29.1.112

[28] Yusof, Mohd Reeza, Mohd Nasrun Mohd Nawi, and Izatul Laili Jabar. "The Absence of Smart Technology as One of The Key Factors of Transportation in Modular Construction: A Case Study in Malaysia." Journal of Advanced Research in Applied Sciences and Engineering Technology 30, no. 1 (2023): 264-274. https://doi.org/10.37934/araset.30.1.264274

[29] https://www.msig.com.my/business-insurance/products/cyber-safeguard/