DOI: https://doi.org/10.33103/uot.ijccce.22.4.3

Systematic Review on Cyber-Security Applications

Shaymaa Mahmood Naser [1], Yossra Hussain Ali [2]
[1,2] *Computer Sciences Department, University of Technology, Baghdad, Iraq*
[1]*cs.19.29@grad.uotechnology.edu.iq,* [2]*yossra.h.ali@uotechnology.edu.iq*

Abstract— *Cybersecurity systems have been taken into account in modern information systems and methods. This is due to the increase in electronic attacks on storage information in terms of transmission, reception and storage. Therefore, the need to produce such systems in a complete way to prevent their penetration into the network has increased. In addition, artificial intelligence (AI) methods are used in cybersecurity systems as classifiers, attack detectors, and components for predicting threats that surround the network. This requires more information about threats and vulnerabilities to be covered to avoid any errors. In this paper, a systematic review is conducted to cover cybersecurity used in various applications, including systems based on wireless, cloud, and mobile sensor networks (WSN). The systematic review approach is adopted on a two-way basis to produce a clear view of the research work to date and to provide a field that can be used for future work.*

Index Terms— *WSN, Cyber-Security, Cyber Applications, AI.*

I. INTRODUCTION

Over the recent years, the cyber issues have been noticed in different information systems that are related to software and hardware sides. It is well known that the cyber-security includes numerous phases, such as authentication and encryption. It also completes the Cyber Physical Systems (CPS) to be more safe [1]. CPS includes three main parts: physical, communications, and webserver. The physical part is represented by Wireless Sensor Network (WSN) and Internet of Things (IoT) environment. This part is the most attacked part by cyber-attacks due to limitations of abilities of involved nodes and the high verities. Different attacks can destroy the physical part by flooding the information to the network as well as injection fake information [2]. The communication part is represented by the communication systems and related network protocols that are used in data and information exchange. It is the lowest part that attacked by cyber attackers as it uses safe protocols and systems, such as MQTT, http, and TCP protocols as well as WiFi, Bluetooth, ZigBee, LTE and GSM communication systems. The final part of CPS is the webserver that is represented by built website, database, and cloud based services. They send requests to the physical part for sending the sensor readings as packets through the communications part. All received data is stored in the designed database that can be in a server or in cloud [3]. The cyber-attacks are classified according to their functions into numerous types, such Denial of Service (DoS), Distributed (DDoS), and SQL injector. Each cyber-attack has its own run procedure to affect the work of such node and CPS. Group of attacks work on flooding the WSN to increase the congestions and delay as well as packet loss. While another group inject fake information to the network and database [4].

Artificial Intelligent (AI) methods are widely used in the cyber-security system, particularly in detections, prevention and optimized classification of attacks. Different methods of AI are used depending on the application and related circumstances. These methods include deep-learning, swarm intelligence, neural network, and genetic algorithms [5].

In this paper, systematic review of cyber-security applications is presented. This method is adopted to pint out the main aspects of cyber as systems and methods. Throughout this review, the literature research works are classified into different sections depending on the used applications.

Received 22/December/2021; Accepted 08/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.3

II. GUIDELINES FOR PREPARING YOUR PAPER

As mentioned earlier, the systematic review is adopted in showing the related research work so far in terms cyber-security aspects and applications. The applications are divided into different classes to cover all sides as follows:

A. Web applications

In [6], activities of cyber-black hat hackers had been detected in a presented framework that employed Semantic Web Technologies (SWT). This framework extracted and analyzed the text in on-line natural languages. The authors of [7] used a multi-level sequence clustering and machine-learning classifier to detect irregular behavior of the request structure of the adopted HTTP based website. All requests were represented as tokens, used for authentication and identification. In [8], three parts were combined in a cyber-security system including: web projection, web crawler, and autonomous. From the dynamic reconstruction of the collected websites, any cyber-attacks were detected in efficient way. The attacks here represented the web malicious. In [9], an online cyber-security based monitoring system for websites was presented. These websites adopted intelligence analysis for centric data gathering that worked on web logs, browsers and mobile fingerprint. The time factor was considered for detecting the cyber-attacks. Authors of [10] adopted certification algorithm in verifying the Cyber-Physical Systems (CPS) that used different websites. Security component properties were employed to detect the cyber intruders for interface automata. At the other hand, a machine-learning was used in intelligent cyber-threat detection that came from dark websites [11]. The request forum was considered and analyzed for confirming the attacks of cyber in accurate way. In [12], the data level and privacy for HTTP security had been used to assess the websites. The certification method was adopted as well to ensure the authentication and identification of included nodes. In [13] and [14], the cybercrimes had been assessed for official websites, such as universities and business. They studied the possibilities of enhancing the security ability against the cyber-attacks using bird eye and solid barriers methods. While the authors of [15] took care from the websites using intelligent methods, such as deep-learning, CNN, and RNN to detect the cyber-threats. Moreover, a visual interactive platform was proposed for easing the use of the presented cyber-security system.

B. Cloud Applications

It is important to focus on the cyber-security application in the cloud computing based systems. The AI technologies were applied in the cloud computing applications in terms of cyber-security [16]. This was for securing the internet transportation in addition to privacy and data encryption. In [17], a cyber-security framework had been proposed to detect the malicious devices, included in the underlined network. The application was allocated in the fog layer as a protection against intrusions and virtual honeypot technologies based attacks. The authors of [18] presented an overview on the research work that tackled cloud computing cyber-security. It considered the cyber-attacks types as well as all related threats. In [19], the cloud based block-chain roles had been secured against cyber-attacks. As the block-chain information was stored in loud, the privacy, and cyber-security were adopted in the proposed security system to cover the transactions. Moreover, an analytics framework had been financially cyber-secured with the assistance of Monte Carlo simulations to ensure the effective performance in cloud layer. This was done by proposing two algorithms with the help of AI [20]. Another platform for cyber-security for cloud computing application was proposed in [21]. This platform considered the marketing issues in different aspects, including trading, management, and market competition. These aspects were constructed to be secured against the cyber-attacks from cloud server and users sides.

In [22-24], different cloud computing based cyber-security systems were presented as platforms. The systems took care of data and information exchange as well as storage in the institutes of government, such as health and educational ones. This was done using AI technologies in addition to traditional

Received 22/December/2021; Accepted 08/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.3

cyber-attacks detection methods. The authors of [25] presented a cyber-security tools for detecting and minimizing the effects of attacks in Korean government. These tools had the ability in doing training in terms of cyber-security issues that can face cloud based web applications. At the other hand in [26, 27], different methods had been proposed to ensure the security of education systems form cyber-attacks. The aims were to mitigate the effects of cyber-attacks with different types to cover the information safe delivery.

C. Mobile Applications

In the field of mobile applications, the security and particularly cyber one has to be considered in efficient way. Numerous researchers adopted the AI and cyber-security systems in the presented mobile applications. In [28], a review manuscript had been presented to show the types of major problems that faced mobile applications in terms of cyber-attacks. The attacks could include infrastructure and information in these applications. The authors of [29] presented mobile based health care systems that adopted cyber-security methods for social multimedia based on multi-level of cloud services. In addition, the presented cyber-security system in [30] and [31] tackles two sides: malware guardian and password. It meant that it solved the problem of users and server using game theory, which proved its ability in detection and mitigate the security threats. The IoT was adopted as well to represent the data source. In [32], a cyber-crime had been addressed for mobile applications. The proposed system considered the attacks for information in the mobile network, where the attackers could send malicious codes to the main system for destroying purpose. At the other hand, behavior dynamic and static analysis for mobile application had been adopted in [33] to detect the cyber-attacks from unknown devices.

In [34], cyber-attacks had been detected and addressed using the proposed cyber-security system. These attacks included DoS, SQL injection and DNS. The authors of [35] studied the effects of increasing the population in mobile using, in which the cyber-attacks can also increase. They considered the cyber-crime in different fields of mobile applications and the ways of detection and prevention of threats. In [36] and [37], the cyber security challenges and related malwares had been analyzed and classified for different mobile applications, such as banking.

D. WSN Applications

Numerous applications have been listed in the literature over last years. This is due to the importance of WSN in real life that are presented as solutions for a lot of problems, especially in emergencies and monitoring systems. The applications of WSN varied from architecture to oil production to system management to smart housing to traffic control to heath monitoring, and so on [38-47].

Security in WSN has become as trending point by researchers due of the high importance of the exchanging data and information. Different research work had been presented in this field to deal with the offering a safe route between the source and destination of WSN, whereas it was cluster based or not [48] and [49]. In Cyber Physical Systems (CPS), the WSN is the base of physical level. This level suffers from different types of cyber-attacks. These attacks destroy the designed system and can inject fake data and information inside the system. In [50] and [51], comprehensive studies and assessments for cyber security side in WSN was presented. In addition, the communications level in WSN was considered to be used in attack detection. The authors of [52] and [53] presented a new method of cooperative security key generation in WSN as a part of CPS. The fading channel randomness was adopted to generate the key. Moreover, the recent communication standards as well as the cyber-attacks for WSN had been included. In [54], a CPS is simulated using virtualization tools to represent the work of sensors that can be attacked in cyber way.

At the other hand, SDN and WSN had shared a collaborative security framework in detection of cyber-attacks and threats [55]. It was designed for lightweight intrusion prevention aspects. In [56], the RF based WSN was considered in autonomous vehicle system that used cyber-security method for preventing attacks. IoT protocols were applied to reduce the challenges in managing vehicle system. The cyber-security was used in enhancing the privacy of exchanged information in the system. Authors of [57] proposed a cyber-security method to mitigate the effects of attacks, particularly for low-power IoT devices. The low powered devices reduced the ability of nodes in WSN in resisting cyber-attacks in wright way. In [58- 60], the cyber-security systems were built in multi-level to save the traffic

Received 22/December/2021; Accepted 08/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.3

VANET for police car. The presented cyber systems tackled DoS attacks that can destroy the VANET and fuzzy the system with fake information regarding the traffic congestion points.

E. Goverment Applications

Due to the high important of employing cyber-security system in the applications of different fields. Applications that used by government around the world, adopt cyber technologies in order to prevent the related attacks. In [61], most of the standard roles, and regulations of cyber-security, used by governments, and its aspects had been explained. It considered the framework recommendations as well for junior users in cyber-security. All challenges of these system were listed as well. In addition, the agency information systems for managing the strategies of different governments were proposed in[62]. The cyber-security and related effected factors were studied and analyzed to produce tools for collaborating the agencies over different fields. In education level, the strategy of building a cyber-security course was produced in [63] and[64]. The included divisions of academia were classified according to the need of cyber-security course. Moreover, the risk of losing the information was reduced to cover the requirements. The authors of [65] produced a roadmap for five years to build and improve the cyber-security algorithms used by the government. The building was based on responsibilities and standards of developments. In [66], cyber hygienic protocols were proposed to address the critical dangerous of cyber-crime in the time of COVID-19. Governments adopted these protocols in education, health and other fields to compensate the lack of information and to keep the accuracy high. At the other hand, different aspects of cyber-attacks had been presented in[67]. These aspects included critical infrastructure attacks, analyzes attack vectors and attack methods. They were used to manage the government requirements in terms of information security. In [68] and [69], the intelligent methods had been used in building Governments' strategical planning with less effects of cyber-security attacks on the underlined information systems. Authors of [70] produced reported list of agency readiness from more than thirty Governments to recover the effects of disasters on the information systems. Different statistical studies using SPSS system were introduced to study the effects in deep look. In colclusions, the research work sor far [6]-[70] can be summarized in Table I.

TABLE I: RESEARCH WORK [6]-[70] COMPARISON.

Research Work	Applications	Technologies	Drawbacks
[6]-[15]	Web Applications	1. Deep_learning. 2. Machine Learning. 3. Monitoring technology. 4. Website frameworks. 5. Website assement technology.	1.Lack of database security. Authors neglegte the security of data inside the database, while a lot of attacks can dameges it. 2.Absence of attack prediction, while the presented methods dtetcted the cyber-attacks in low accuracy ratios.
[16]-[27]	Cloud Application	1. Cloud based platforms. 2. AI methods. 3. Cloud security. 4. Block-chain security technology. 5. Monitoring technology.	1. The low security connection between cloud and web apploication. The trasactions of data within the network was not covered to produce more secure system. 2. Excluding the security from available cloud services. The security in cloud services is hgihgly important and shuld be condider to present secured

Received 22/December/2021; Accepted 08/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.3

			systems to avoid the absence of a comperhansive cyber-security system.
[28]-[37]	Mobile Applications	1. Maleware and thread detection technologies. 2. Statical evlauations. 3. Mobile security.	1. Authors neglected the security of data exchange between the mobile application nd related wesites that can be used to store the data. 2. High complexity security system to be implemented in mobile devices. The complexity was the results of using multi-techniques of secuirity. 3. Absence of a comperhansive cyber-security system that delt with all mobule network layers
[38]-[60]	WSN Applications	1. DoS detection. 2. Security assessment. 3. WSN protocols. 4. Authentication methods. 5. Encryption methods.	1. Lack in presenting security system that control the data transmition in safe. 2. Authors presented a complex application to be implemented on limited resources WSN. 3. Absence of Cyber-predection system that can prvenet most of attacks in early stages. 4. Problems of mobility and clustering were not tackled to be considered in the presented system.
[61]-[70]	Government Applications	1. Standrization of roles. 2. Stratigical planning. 3. Data applications. 4. High security data transfer.	1. These systems considered parts of the whole secuiryt systems and neglegted others. 2. Authors did not consider the early stage of attack prediction.

III. PROSPECTIVE CYBER-SECURITY SYSTEM

As explained above, the information systems for different applications require strong security systems that can guarantee, with high ratio of security, the safe of included data. Therefore, it is important to figure out and highlight the aspects of producing these systems.

By considering the systematic review in this paper, *Fig. 1* shows the classifications of the research work in literature as a block diagram. The adopted structure is the heretical shape from wide base to narrow, in which the important fields are covered and explained well.

This figure shows the applications of cyber-security systems as a wide base, and then considers the specific areas step by step according to the research work in literature [6, 70]. These systems in literature suffered from drawbacks that varies from heavy to light as follows:

1. The most important problem is the accuracy of detecting the cyber-attacks.
2. Clear lack in cyber-attack prediction.
3. Neglecting important concepts, such as the development of cyber-attacks, in which smart methods are proposed and considered.
4. The availability of comprehensive cyber-security systems for WSN.

Received 22/December/2021; Accepted 08/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.3

The pink highlighted blocks represent the hot area that are the considered by the prospective cyber-security system in this paper. These areas are based on combining the AI, cyber-security, and WSN for producing a comprehensive security system with high efficiency in tackling different types of cyber and normal attacks in WSN, which is a part of CPS. To be more precise, the following aspects should be considered and contributed for prospective cyber-security systems for WSN:

1. Producing cyber-security system that has detection algorithm for discovering the current and active cyber-attacks on the WSN.
2. Moreover, a prediction algorithm should also be proposed to expect the worst in case of weakness happened in the underlined security system.
3. Using AI methods in producing the detection and prediction algorithms of point 1. This is to increase the accuracy of detecting and predicting procedures of cyber-attacks.
4. Combing the produced algorithms and methods in a comprehensive cyber-security system for WSN.
5. Evaluating the performance of produced methods in regular way to ensure that the system is working well with high efficiency in terms of detecting and predicting the cyber-attacks.

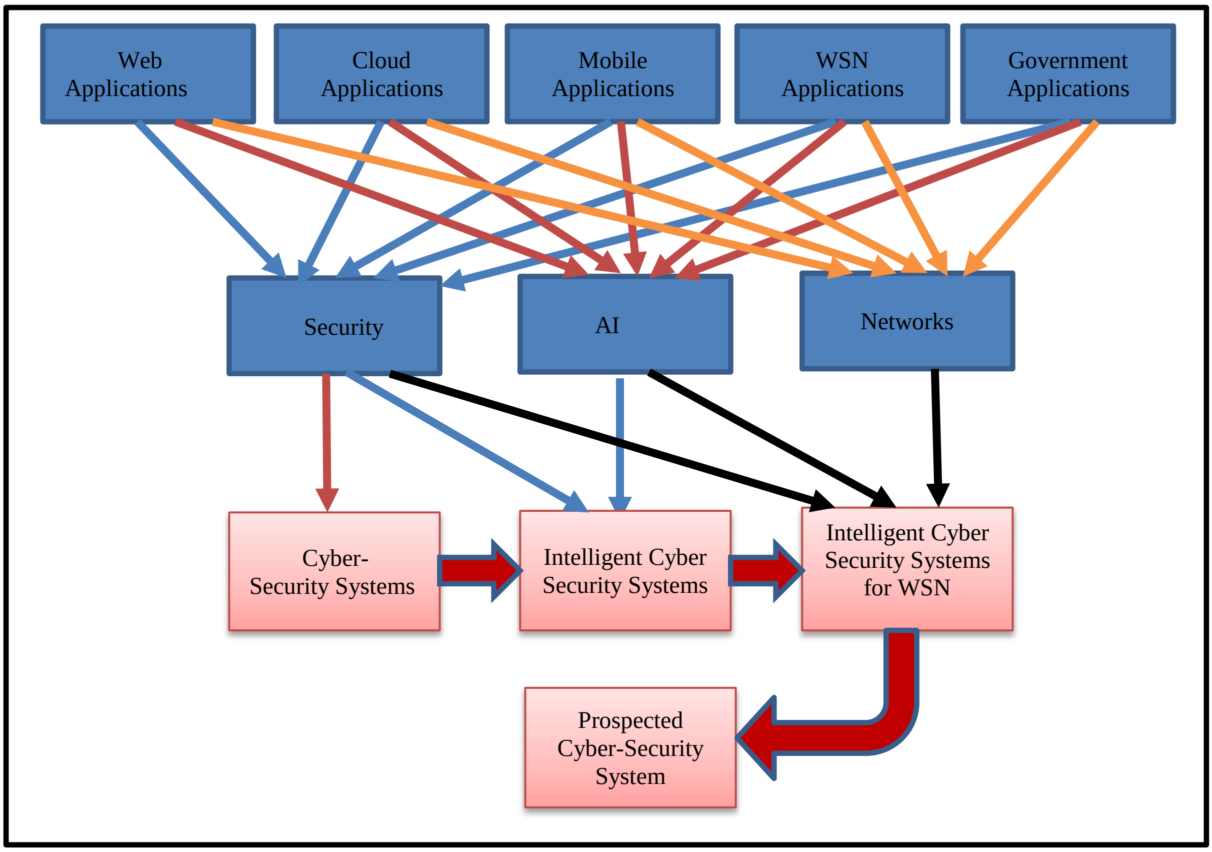

FIG 1. SYSTEMATIC REVIEW FOR PROSPECTIVE CYBER-SECURITY SYSTEM.

IV. CONCLUSIONS

This paper presented a systematic literature review of cyber-security system for CPS and particularly for WSN. This was to point out the drawbacks and weak joints of producing a strong security system for important applications including WSN. Based on the research works in literature with the assistant of systematic methodology, a prospective cyber-security system for WSN was presented. This system covered the lack points of previous work and compensated the missing joints that can be gates for cyber-attacks. The prospective system considered the AI methods for increasing the accuracy of detecting the cyber-attacks. This accuracy helped the applications in avoiding the loosing of services by attacks in early stages.

Received 22/December/2021; Accepted 08/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.3

Moreover, the prospective cyber system adopted the cyber-attacks prediction that can produce a really strong WSN applications that can resist these attacks before happening. The expected results can increase the resilience of the prospective cyber-system against attacks in efficient way to be used for different WSN applications. For future business advice suggests standardization frameworks new protocol designed for cyber-security in WSN contain suggest more than one AI algorithm surmise that expected cope bad cases if hung the system suddenly, then reform the execution of processes for ensuring the system is well.

REFERENCES

[1] P. Marwedel, Embedded System Design, Systems Foundations of_Cyber-Physical Systems, an the_Internet of_Things, Springer, Fourth Edition, 2021.

[2] F. Hu, Cyber Physical System Integrated Computing and Engineering Design, Taylor and Francis Group, 2014.

[3] H. Song, G. A. Fink, S. Jeschke, Security and Privacy in Cyber-Physical Systems",Foundations, Principles, and Applications Wiley-IEEE Press, 2018.

[4] H. Song, D. Rawat, S. Jeschke, and C. Breche, Cyber-Physical Systems, Academic Press, 1st Edition, August 2016.

[5] S. Kremer, L. Mé, D. Rémy, and V. Roca, Cybersecurity : Current challenges and Inria's research directions, WHITE BOOK ,No. 3, January 2019.

[6] T. Georgescu, and I. Smwureanu, "Using Ontologies in Cybersecurity Field", Informatica Economică, Vol. 21, Mar 2017.

[7] R. Kozik, M. Chora's,and W. Holubowicz, "Packets tokenization methods for web layer cyber security", Logic Journal of IGPL, Vol. 25, No. 1, Aug 2016.

[8] Y. Kawano, and E. Nunohiro, "A Proposal of Distributed Autonomous Cooperative System about Exclusive Web Crawling for Cyber Security ", IEEE19th International Conference on Network-Based Information Systems, 2016.

[9] C. Onwubiko, "Exploring Web Analytics to enhance Cyber Situational Awareness for the Protection of Online Web Services", International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), 11 Jul 2016.

[10] C. Sun, Q. Yao, and J. Ma, "Certia: Certifying Interface Automata for Cyber-Physical Systems", International Conference on Smart Computing (SMARTCOMP), Jun 2017.

[11] M. KADOGUCHI, S. Hayashi, M. Hashimoto, and A. Otsuka, " Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning", International Conference on Intelligence and Security Informatics (ISI), Sep 2019.

[12] S. Wibowo, J. Indonesia, "Enriching Digital Government Readiness Indicators of RKCI Assessment with Advance Https Assessment Method to Promote Cyber Security Awareness Among Smart Cities in Indonesia", International Conference on ICT for Smart Society (ICISS), Nov 2018.

[13] A. Kassem, A. Al Hajjar, B. Daya, P. Chauvet, "A Proposed Methodology for Cyber Security Mechanism according to the most popular detected attacks for University Web Application", Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), Jan 2019.

[14] M. Kannan, "A Bird's Eye View of Cyber Crimes and Free and Open Source Software's to Detoxify Cyber CrimeAttacks– an End User Perspective", IEEE 2nd International Conference on Anti-Cyber Crimes (ICACC), Apr 2017.

[15] R. Williams, S. Samtani, M. Patton, and H. Chen, "Incremental Hacker Forum Exploit Collection and Classification for Proactive Cyber Threat Intelligence: An Exploratory Study", IEEE International Conference on Intelligence and Security Informatics (ISI), 2018.

[16] B. Richardson, "Cyber Security and Artificial Intelligence for Cloud-based Internet of Transportation Systems", 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Aug 2020.

[17] A. Sohal, R. Sandhu, S. Sood, and V. Chang, "Cybersecurity Framework to Identify Malicious Edge Device in Fog Computing and Cloud-of-Things Environments", Computers & Security, Vol. 74, pp. 340-354 , 2018.

[18] H. Bennasar, A. Bendahmane, and M. Essaaidi1, "An Overview of the State-of-the-Art of Cloud Computing Cyber-Security", Springer International Publishing, pp. 56–67, 2017.

[19] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy", Telecommunications Policy, Vol. 41, No. 10, pp. 1027-1038, Nov 2017.

[20] K. Gai1, M. Qiu, H. Hassan, "Secure cyber incident analytics framework using Monte Carlo simulations for financial cybersecurity insurance in cloud computing", Concurrency and Computation Practice and Experience, Jan 2016.

[21] D. Arce, "Cybersecurity and platform competition in the cloud", *Computers & Security*, Vol. 93, Jun 2020.

[22] M. Frank, M. Leitner, and T. Pahi, "Design Considerations for Cyber Security Testbeds: A Case Study On a Cyber Security Testbed for Education", IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intel Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Apr 2018.

Received 22/December/2021; Accepted 08/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.3

[23] T. Tareke, and S. Datta, "Automated and Cloud Enabling Cyber Security Improvement in Selected Institutions/Organizations", Second International Conference on Computing Methodologies and Communication (ICCMC), Oct 2018.

[24] W. Nie, X. Xiao, Z. Wu, Y. Wu, F Shen, and X. Luo, "The Research of Information Security for The Education Cloud Platform Based on AppScan Technology", 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Jul 2018.

[25] Y. Park, C. Choi, C. Jang, D. Shin, G. Cho, H. Kim, "Development of Incident Response Tool for Cyber Security Training Based on Virtualization and Cloud", International Workshop on Big Data and Information Security (IWBIS), Dec 2019.

[26] S. Puri, and M. Agnihotri, "A Proactive Approach for Cyber Attack Mitigation in Cloud Network", International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017), Jun 2018.

[27] N. Patala, A. kadyamatimba, and S. Madzvamuse, "Adoption of Cloud-Cyber Security: Challenges and Perceptions Within Resource Constrained Higher Education Institutions", Open Innovations Conference (OI), Nov 2018.

[28] A. AlDairi, L. Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies", International Workshop on Smart Cities Systems Engineering (SCE 2017) , Procedia Computer Science, Vol 109, pp. 1086-1091, 2017.

[29] J. Al-Muhtadi, B. Shahzad, K. Saleem, W. Jameel, and M. Orgun, "Cybersecurity and Privacy Issues for Socially Integrated Mobile Healthcare Applications Operating in A Multi-Cloud Environment", Health Informatics Journal, Vol. 25, No. 2, pp. 315–329, 2019.

[30] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "Enhancing Cyber Security Awareness with Mobile Games", The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017), May 2018.

[31] J. Abawajy, S. Huda, S. Sharmeen, M. Hassan, and A. Almogren, "Identifying Cyber Threats to Mobile-IoT Applications in Edge Computing Paradigm", Future Generation Computer Systems, Vol 89, pp. 525-538, Dec 2018.

[32] S. Vashisht, S. Gupta, D. Singh, and A. Mudgal, "Emerging Threats In Mobile Communication System", IEEE1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016), Aug 2016.

[33] A. Arabo, "Mobile App Collusions and its cyber security implications", *IEEE 3rd International Conference on Cyber Security and Cloud Computing*, Aug 2016.

[34] Suhasini Sodagudi, Sita Kumari Kotha, M.David Raju, " Novel Approaches to Identify and Prevent Cyber Attacks in Web", IEEE 3th International Conference on Computing Methodologies and Communication (ICCMC 2019), Aug 2019.

[35] E. Stones, Mobile Communications: M-Crime and Security, Ph.D. Thesis in Security and Crime Science, Department of Security and Crime Science, University College London, Jun 2017.

[36] N. Wechuli, W. Franklin, and W. Jotham, "Cyber Security Challenges to Mobile Banking in SACCOs in Kenya", International Journal of Computer (IJC),Vol. 27, No. 1, pp. 133-140, 2017.

[37] A. Arabo, and B. Pranggono, "Mobile Malware and Smart Device Security: Trends, Challenges and Solutions", IEEE 19th International Conference on Control Systems and Computer Science, 30 Jul 2013.

[38] N. Mossa, W. Shareef, F. Shareef, "Design of Oil Pipeline Monitoring System based on Wireless Sensor Network", Iraqi Journal of Computers, Communications, Control and Systems Engineering (IJCCCE), Vol. 18, No. 2, Sep 2018.

[39] Z. Faris, M. Croock, "Drip Irrigation Scheduling System Using Sensor Network", Iraqi Journal of Computers, Communication and Control and System Engineering (IJCCCE), Vol. 17, No. 1, Nov 2017.

[40] M. AL-Zaidi , S. Hussein Al-Samarae, "Employing Smart Systems in Integrated Management of Infrastructure for Housing Projects", Iraqi Journal of Architecture and Planning, Vol. 19 , No 2, PP. 72-87, Dec 2020.

[41] H. Hassan, N. Hadi, "Implementation of Wireless Area Network for Patient Monitoring System", Iraqi Journal of Computers, Communication and Control and System Engineering (IJCCCE), Vol. 17, No. 1, Nov 2017.

[42] H. Hassan, A. Rasheed, H. Abdulkareem, "Implementation of Workshop Air Pollution Monitoring System Based On Wireless Sensor Network", Iraqi Journal of Computers, Communication and Control and System Engineering (IJCCCE), Vol. 19, No. 4, Oct 2019.

[43] W. Alzubaidi, S. Shaker, "Secure Routing Scheme for Clustered Wireless Sensor Network (WSN)", Interciencia Journal, Oct 2018.

[44] A. Khlaif, M. Croock, and S. Shaker, "Simulating Traffic Lights Control using Wireless Sensor Networks", International Journal of Computer Applications, Vol. 104, No. 12, Oct 2014.

[45] A. Khlaif, M. Croock, S. Shaker, "Traffic Lights Control using Wireless Ad-Hoc Sensor Networks", IJCCCE, Vol. 15, No. 1, 2015.

[46] R. Yas , and S. Hashem, "A Survey on Enhancing Wire/Wireless Routing Protocol Using Machine Learning Algorithms", IOP Conference Series: Materials Science and Engineering, 2020.

[47] R. Yas, and S. Hashem, "Unequal clustering and scheduling in Wireless Sensor Network using Advance Genetic Algorithm", Journal of Physics: Conference Series, 2020.

[48] W. ALzubaidi, S. Shaker, "Efficient Cluster Head Selection and Optimized Routing in Wireless Sensor Network(WSN)", Journal of Theoretical and Applied Information Technology, Vol. 97, No. 4, Feb 2019.

Received 22/December/2021; Accepted 08/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.3

[49] W. Alzubaidi, and S. Shaker, “Methods of Secure Routing Protocol in Wireless Sensor Networks”, Journal of AL-Qadisiyah for Computer Science and Mathematics, Vol. 10, No. 3, 2018.

[50] L. Chhaya, P. Sharma, G. Bhagwatikar, A. Kumar, “Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control*”*, Electronics,Vol. 6 , No. 1, 2017.

[51] D. He, S. Chan, and M. Guizani, “Cyber Security Analysisand Protection of WirelessSensor Networksfor Smart Grid Monitoring”, IEEE Transection on Wireless Communications, Vol. 24, No. 6, Dec 2017.

[52] K. Li, H. Kurunathan, R. Severino, and E. Tovar, “Cooperative Key Generation For Data Dissemination in Cyber-Physical Systems”, IEEE 9th ACM/IEEE International Conference on Cyber-Physical Systems, Aug 2018.

[53] A. Burg, A. Chattopadhyay, K. Lam, “Wireless Communication and Security Issues for Cyber– Physical Systems and The Internet-of-Things”, Proceedings of the IEEE, Vol 106, No 1, Jan 2018.

[54] Y. Cai, “Group Communication for Configurable Virtualized Sensors in Cyber-Physical Computing Environment”, International Conference on Computer Communication and Network Security (CCNS), Nov 2020.

[55] C. Miranda, G. Kaddoum, E. Bou-Harb, S. Garg, and K. Kaur, “A Collaborative Security Framework for Software-Defined Wireless Sensor Networks”, IEEE Transcations on Information Forensics and Security, Vol. 15, Feb 2020.

[56] H. Garakani, B. Moshiri, and S. Safavi-Naeini, “Cyber Security Challenges in Autonomous Vehicle: Their Impact on RF Sensor and Wireless Technologies”, 18th International Symposim on Technology And Applied Electromagnatic (ANTEM) , Dec 2018.

[57] A. Bandekar, A. Javaid, “Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices”, 7th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, Jul 2017.

[58] M. Yasir, M. Croock, “Multi-Level Cyber Security System for VANET”, Indonesian Journal of Electrical Engineering and Computer Science, Vol. 19, No. 2, pp. 940-948, Aug 2020.

[59] M. Yasir, M. Croock, “Cyber DoS Attack-Based Security Simulator for VANET", International Journal of Electrical and Computer Engineering (IJECE), Vol. 10, No. 6, pp. 5832-5843, Dec 2020.

[60] M. Yasir, M. Croock, ”Software Engineering Based Self-Checking Process for Cyber Security System in VANET”, International Journal of Electrical and Computer Engineering (IJECE), Vol. 10, No. 6, pp. 5844-5852, Dec 2020.

[61] J. Srinivas, A. Kumar Das, and N. Kumar, “Government Regulations in Cyber Security: Framework, Standards and Recommendations”, Future Generation Computer Systems, Vol. 92, pp. 178-188, Mar 2019.

[62] J. Tama, “How An Agency’s Responsibilities and Political Context Shape Government Strategic Planning: Evidence from US Federal Agency Quadrennial Reviews”, Public Management Review, Journal homepage: http://www.tandfonline.com/loi/rpxm20, 2017.

[63] T. Pereira, “Challenges and Reflections in Designing Cyber Security Curriculum”, IEEE World Engineering Education Conference (EDUNINE), May 2017.

[64] J. Kim, S.Winds, “Cyber-Security in Government: Reducing the Risk”, Computer Fraud & Security, Jul 2017.

[65] J. Johnson, “Roadmap for Photovoltaic Cyber Security”, Sandia National Laboratories, Dec 2017.

[66] A. Abukariand, and E. Bankas, “Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond”, International Journal of Scientific & Engineering Research Vol. 11, No. 4, Apr 2020.

[67] T. Limba, T. Plėta, K. Agafonov, and M. Damkus, “Cyber Security Management Model for Critical Infrastructure”, The International Journal, ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES, Vol. 4, No. 4, Jun 2017.

[68] T. Thomas, A. Vijayaraghavan, and S. Emmanuel, Machine Learning Approaches In Cyber Security Analytics, Springer Nature Singapore Pte Ltd. 2020.

[69] X. Feng, Y. Feng, E. Dawam, “Artificial Intelligence Cyber Security Strategy”, Congress of IEEE, Nov 2020.

[70] H. Lantto, B. Åkesson, M. Sci, J. Kukkola, J. Nikkarila, M. Ristolainen, “Wargaming A Closed National Network: What Are You Willing to Sacrifice?”, Cyber Security and Trusted Computing,Vol. 3, 2018.

Received 22/December/2021; Accepted 08/April/2022