Journal of Engineering and Applied Sciences
MEDWELL PUBLICATIONS

Technology Development Through Change in Cybercrime of Smart Devises

Mohammed I. Alghamdi
Department of Computer Science, Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia

Key words: Cybersecurity, network security, various, amount, regard

Corresponding Author:
Mohammed I. Alghamdi
Department of Computer Science, Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia

Page No.: 2834-2840
Volume: 15, Issue 14, 2020
ISSN: 1816-949x
Journal of Engineering and Applied Sciences

Abstract: The smart city is a phenomenon, constantly evolving and expanding and soon becomes a model for transforming connected cities. More and more parts of cities are connected and with it, risks and issues are increasing. However, smart city projects often ignore the dangers and threats of cybersecurity that pervade these initiatives. This research study aims to explore and identify the various factors that affect the lack of focus on cybersecurity in smart cities. The study found multiple factors that have implications for the amount of focus on cybersecurity. The study identifies a complex web of factors that lack cybersecurity in smart cities that have a multi-directional impact on each other. The study also acknowledges that there is a fundamental problem with regard to the level of adequate cybersecurity but indicates that the current focus on cybersecurity is a reaction rather than a proactive which creates innate and critical problems for the future.

INTRODUCTION

Smart cities is a very contemporary phenomenon with huge amounts of resources and time spent developing various areas of application using connected technology[1]. The main objective of these projects is to improve the quality of life for the urban population and it comes in response to the many different problems that come with the densely populated urban areas. The smart city as a phenomenon practiced three decades ago was developed and practiced. Smart city projects differ in their application areas from connected waste bins to "smart" building automation devices[2, 3].

Although, the term "smart city" is referred to and used extensively, it is a surprising challenge to precisely define the boundaries of this concept which is agreed by many. Despite this, Carrie, etc., the concept of smart cities is defined as "a complex system of social and technical systems" which will be appropriately named as a constellation of systems in this research. Yadav, etc. describe smart city as a concept where difficult city issues are addressed by integrating Information and Communications Technology (ICT) with urban city infrastructure in order to create a fair and sustainable system[3].

There are many broad spectrum initiatives from high examples like the European Union called the European Initiative on smart cities but also smaller ones like EU and Smart City Sweden. The main focus of these initiatives is on finding sustainable and smart city solutions[1-5].

The potential for increased luxury with smart city initiatives is great and can be applied to different regions as mentioned earlier. Examples range from more efficient traffic flows, more efficient waste management and less energy consumption, especially in both housing and offices which is seen as an incredible decrease in energy

consumption as buildings generally make up two-thirds of overall energy consumption. Zanella, etc., presents the explanation that smart cities aim to improve and be part of a wide range of new services provided to citizens and companies as well as public administrations. They argue that automation in both homes and industries as well as medical and elderly assistance, smart energy management and smart grids will be affected and more effective[4].

Many believe that the "smart society" we are moving towards is similar to the one found in science fiction movies and other cultural means, something Chakravorty and Chaturvedi describe as somewhat far-fetched as it is no less vital. Instead, they conclude that smart city projects are more subtle in the way they affect our daily lives in various beneficial and current ways. Chakravorti and Chaturvedi claim that there are three main outcomes for smart city projects, namely; General welfare of urban citizens, increased institutional efficiency and a more robust economy[5].

Zanella etc. confirms that smart cities are based on Information and Communication Technology (ICT) as well as Internet of Things[6] devices. They recall that IoT devices and everyday objects full of "microcontrollers, digital communication transmitters and receivers and appropriate protocol stacks" have had a revolutionary impact and are a model for the future. The goal, they said is to achieve a more comprehensive and widespread internet. However, they concluded that there is a lack of unified policies and best practices due to their "modernity and sophistication" which must be overcome in order to achieve a bright future for smart cities[7].

CYBERSECURITY

According to the International Telecommunication Union (ITU-T, 2008), cybersecurity is defined as follows: "Cybersecurity is a set of tools, policies, security concepts, security guarantees, guidelines, risk management approaches, procedures, training, best practices, warranties and technologies that can be used to protect the cyber environment, enterprise and user assets." Moroccan and Lucavio define cybersecurity in terms of cybersecurity in this way; "Security includes unlawful access to information and attacks that cause physical disruptions in service availability".

Cybersecurity is often similar to the term information security and used together to describe the security of an organization's information infrastructure. Von Solms and van Niekerk argue that while the two concepts are very similar, they are not exactly the same. Instead, they point out that cybersecurity includes another dimension of security which is the dimension of defending human lives from cyber attacks which is very recent due to the spread of information systems in critical infrastructure, especially in urban areas of the smart city where accidents may affect the lives of Humans are passively[8].

Our interpretations of the two terms are very similar given the nature of the research area in this study. By protecting information systems in smart city applications (information security), human life is likewise more secure (the additional aspect of cybersecurity) that takes into account the physical operation of these systems in the real world. We are therefore expanding the scope of information security in the application of smart city contexts which then become similar to cybersecurity due to the latter's goal of protecting human lives[9].

Smart city initiatives are often associated with increased connectivity via connected devices that are often called "Internet of Things". Internet of Things[6] devices described by Jin etc. as excellent data collection tools and delivering this data to a central location for further use. The internet of Things is often found as sensors or actuators-they can control and control simple things in the "real world" with a digital command[8].

As with almost all new technologies, there are of course disadvantages. Many argue that the main reason is the fact that interconnected society and everyday life leave more openness to being digitally attacked in a new category of crime called "cybercrime". One thing that is attributed to the Internet of Things is insecurity and EY is mentioned in the Hardware Insecurity Report as an unsafe feature in smart city communities. Potoczny-Jones also argues about the insecure ways of the Internet of Things, arguing that the Internet of Things has chosen "the lowest fruits of security" which are passwords that have led to massive attacks using hacked devices as slaves who refuse Distributed Distributed attacks (DDoS) like Mirai and new huge robots Recently discovered.

Cybersecurity incidents appear to be occurring with increasing frequency and there are multiple examples related to smart cities. A recent example is an accident in 2011 in which a water pump was destroyed by a cyberattack on a city water station in Springfield Township, Illinois. Another example also occurred in the United States that targeted Dallas and Texas and attackers took control of the city's sirens and proceeded to activate it for several hours during the night. Another more serious example of life is found by an employee of Kaspersky Labs, Denis Legezo. During an investigation into the security of connected traffic lights, he succeeded in his attempt to penetrate and enter traffic lights in central Moscow, giving him full control over the mentioned traffic lights[6].

An example of the Internet of Things and the risk of contamination from unsafe devices for everyone as a whole occurred earlier this year as hackers managed to hit

and penetrate the fish tank thermometer in the hallway and were able to access the casino and export a high-cylinder database[3].

Pearce Anderson highlights many different challenges for smart cities to overcome and include information security as one of these as well as one of the three most common challenges in the field of technical challenges. They mentioned that smart cities will need urban systems that achieve and support interoperability at a high level due to the integration of information and communications technology and the Internet of Things. Given the extreme complexity and interdependence of these systems, Al-Diri and Tawalbeh see a greater attack area for malicious actors[6].

John-Green and Watson state that there is an excessive connection between IoT devices and urban systems and they acknowledge that this involves various problems which they address in four different characteristics, namely excessive communication, loss of borders, ITI complexity and industrial piracy[2].

Smart city and cybersecurity: When conducting a comprehensive review of the literature, we found that the lack of an appropriate and standard definition of the concept of smart city and its components became the first goal. Next, this paper explores the cybersecurity of the Internet of Things devices which are widely used and vital for smart cities[11].

In smart city initiatives, project leaders are not considered a cybersecurity challenge and since no research has been done exploring the reasons behind not specifically focusing on smart city projects, this study has yielded a framework of various potential factors that lead project leaders to lack focus[8].

Smart city: The concept of smart cities lacks a common definition which leads to a variety of smart city definitions. Yadav etc. describes smart cities as a concept that addresses difficult city issues with the help of advanced information and communications technology (information and communications technology), urban infrastructure, citizens and city managers in order to create an equal and sustainable city. Moreover, Carrie etc. describe smart cities as a "complex technical social systems system". Baccarne, etc., describe smart cities as the city of the future with digital technologies that enable cities to become greener, more accessible and more liveable[11].

The perception of this study on smart cities is that as Harrison and others have mentioned that smart cities include cities that link physical, social and commercial infrastructure and information technology to take advantage of the intelligence of the city as a whole. Moreover, the overall goal is to improve the quality of life and operational efficiency with the help of emerging technology. Thus, the three components of operating smart city initiatives are physical infrastructure, social infrastructure and technology[12].

The next section will describe these three components in more detail in order to clarify the meaning of each component. Physical infrastructure can include for example, roads, bridges, water, energy and airports. Social infrastructure consists of resources that help education, health care, intellectual capital and social capital. Finally and most importantly in smart cities is the technology component[10].

Notable municipalities have taken advantage of technology to create efficient services for their citizens through the use of sensors, data storage devices, computers and comprehensive analysis. The researchers describe the Internet of Things[6] as a fundamental pillar of smart cities which provides the possibility to create an urban information framework that provides interoperability between services in the city. Wireless and broadband as well as service-oriented information systems, etc. are vital to harness the collective intelligence of smart cities[2].

However, as mentioned by Pierce and Andersson technology, it's not the only goal of smart cities alone. Instead, technology is a way to support the complementarity of other elements involved in achieving the stated goals. Nam and Bardo say smart city initiatives require judgment-based urban planning with stakeholders[13].

Stakeholders and institutional preparations for it to be successful. Moreover, global sustainability is expected to adopt an international and cross-border approach in order to link companies and regions with success. Mauser, etc., likewise describes that global sustainability is created in the interaction between civil society, governments and other stakeholders and does not derive solely from science. Thus, this study argues that smart city initiatives are leverage through city-to-city cooperation in line with Pierce and Anderson, Mauser etc. and Attour etc. description[14].

Actors in the smart city: Although, the components of smart cities are fairly straightforward, the actors involved are not always clear. Yadav etc. describes citizens as decisive actors in the context of the smart city. Moreover, Damiri etc. also argue that in order to empower smart cities, citizens play a vital role for the necessary social and technical transformation. That is, citizens are producers and consumers of information that is created in smart cities. Moreover, smart cities aim to increase the quality of life of citizens and therefore, smart city requires comprehensive safety at the highest level to ensure stability of this quality of life. Leydesdorff and Deakin describe three other actors by applying a triple helix

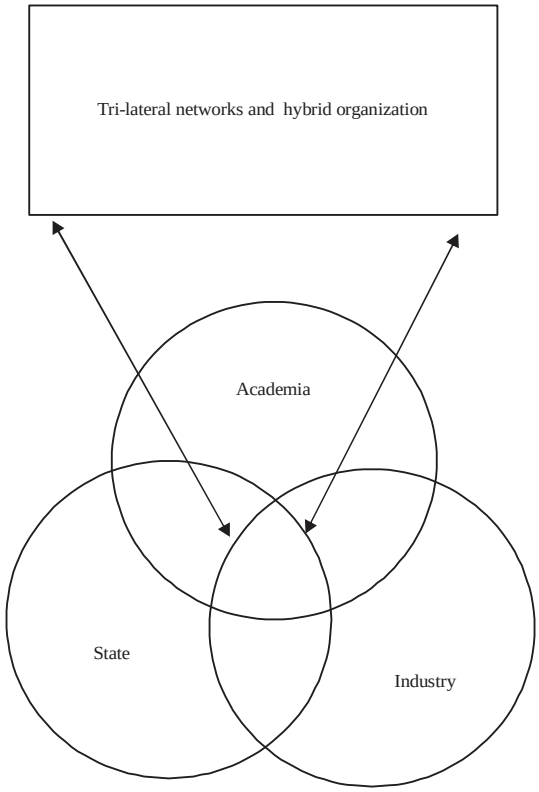

Fig. 1: The triple helix model

model to cities. The researchers explain that the interaction between universities, industries and their governments generates a constantly changing premise for cities. In other words, the overall goal of smart cities set by Harrison and others a description of the three components of the smart city initiative; physical infrastructure, social infrastructure, and technology. The four actors collaborating with the specific components to address the challenges of increasing urbanization are; Government, industries, universities and civil society (Fig. 1).

SMART CITY AND THE INTERNET OF THINGS

Elmaghraby and Losavio claim that the Internet of Things and smart cities are closely interlinked and Baig etc. he argues that the Internet of Things is an enabling technology innovation associated with cloud platforms. The way these devices communicate is by machine-to-machine communication. Klinpratum etc. confirms that M2M connections are essential to the existence of the Internet of Things. Cha etc. Note that M2M is the ultimate model in wireless communications and that there is currently a massive increase in M2ME equipment that will continue to increase in the coming years. Potsch, etc., agrees and explains that M2M communication technology is basically machines that communicate with each other without human intervention. They argue that M2M connections will be spread across different fields and areas of application. They state that research and standardization have yet to reach formal conclusions when it comes to the M2M communication structure and the equipment it uses.

Cybersecurity and the internet of things: Jane etc. a framework proposes to integrate the Internet of Things with complete urban ICT systems and notes that there are many problems that must be overcome before opening a whole smart city area. One of these problems is the unsafe features of IoT devices for widespread applicability for use as an industry report issued by EY indicates non-standardization and general insecurity of these devices which leads to an increased risk of potential adversaries to feeding fake data and hacking IoT devices completely, it caused signal failure or interruption of critical services to the population. Baig, etc., he argues that due to the unencrypted common links between board members, operators and wireless sensor networks where all connections are transferred, there is a high risk of security vulnerabilities.

Reason due to the lack of security measures in the Internet of Things devices, Boison, etc., is the reason why in highly competitive markets where products are launched daily, the rapid release of new products with a high customer comfort factor is essential to maintaining competition. In general, security measures tend to cause sharp or annoying steps for users and are generally slower on the market due to the added complexity. Also, mentioned by Boison, etc. It is the unwillingness of consumers/IoT users that do not have a suitable incentive to demand higher security.

This is also something mentioned by Plachinkova, Vo and Alluhaidan as they argue that security features often block the overall satisfaction of device use. This in turn, reflects badly on the seller/brand which in turn affects sales and competitive advantage. Thibodeaux thinks of the same ideas and writes. “While investment in smart technology has increased, many of these innovations are being deployed without rigorous testing and cybersecurity is often ignored.” Also, important is Sven, Torres and Sarigi who claim that new technology is evolving quickly and quickly that makes it difficult for most designers-even designers themselves-to understand, especially the safe side of it.

Another explanation for why most IoT devices are generally unsafe stems from the fact that most IoT devices are relatively small and often have low energy consumption, says Plachinkova, etc,. for this reason, it is difficult to implement additional security and coding features on devices. Laboda and Gillespie assert that the lack of adequate security standards for the Internet of

Things is a major contributor to the general insecurity of the Internet of Things which is also something Boison, etc. and demanding that only with a common and shared set of safety standards, the Internet of Things will take enough safe measures against violations.

Cybersecurity in smart cities: As head of the Cyber Security Department of the Swedish Civil Emergency Agency (Myn- dighetenförsamhällsskyddochberedskap), Richard Ohm highlights that with the increase in public digitization what follows is an increase in vulnerabilities. He writes: "An example of hostility is cyberattacks that target socially important functions. They happen daily and in large numbers. There are few examples where opponents have committed Distributed Denial of Service Attacks (DDoS) with the intent to cause business interruptions, stealing information or encrypting information for the purpose of claiming. With a ransom". Coylebor and Ashrafi as well as Al-Dairy and Tawalbeh, agree with the ruling and Al-Dairi and Talalba claim that with the cumulative increase in digitization in the city, the surface of the attack follows. This stems from the urgent integration of various technologies, systems, networks and more which creates a very complex, interconnected and interconnected network of digital resources. Veraz and Faraz indicate that this is a serious phenomenon. They point to the effect they call a "viral effect in the urban environment", a place where an intrusion entry point provides an opportunity for malicious actors to gain access to another dependent system. They argue that there is a high risk of contamination from the intense and sophisticated communication patterns of a smart urban area. So, an entry point into one single system can be used as an entry point towards the smart city systems constellation in the smart city.

The systems used in the smart city area are often those called SCADA or supervisory control and data acquisition which are essential components of industrial systems. Thibodeaux highlights SCADA systems as a highly volatile and insecure part of smart cities and argues that if these systems are targeted, they are likely to threaten public health and safety and lead to digital city stops. In fact, this creates a problem because SCADA is uniquely secure and does not have many cybersecurity features. They are often prevalent in cities where the infrastructure is relatively outdated and smart city initiatives are implemented on the already existing analog infrastructure which is a matter of master and others. (2017) confirms.

They state that industrial control systems that differ from SCADA systems are often old in rapid technological progress today and therefore lack the appropriate standards of security needed when connected to the Internet, local networks, etc.

They have come to the conclusion that there is an urgent need to take action to enhance security in industrial control systems but they stress that the best and safest way is to get rid of completely outdated systems and implement completely new systems with a more stable and safer engineering system.

Given the complex set of different systems and devices that make up a smart city, they complicate cyber forensics- that is conduct an investigation and analyze the course of events that lead to a cyber-accident, especially cyber-attacks. Baig, etc., claims that this will indeed be a critical part of smart city, something that is also confirmed by both[15]. But they also insist that until now there are still great difficulties in tracking infection and other malicious acts as well as data recovery procedures in smart cities.

In part, this is due to the problem of excessive communication emphasized by John Green and Watson. They declare that "cyberspace will be a vital component for future cities where infrastructures operate on the Internet" and at the same time reminds us that there are many obstacles and difficulties in this matter, stemming from the four different categories in which they divided engineering risks; Overabundance, chaotic complexity, border loss as well as industrial hacking. Moreover, just like the claims made by Ferraz and Ferraz[15], there is a lack of analysis tools and techniques available for smart cities to use to mitigate these threats.

Lack of focus on cybersecurity in smart cities: Despite the fact that cybersecurity is important it has been proven; cybersecurity is crucial to the heavy environment of information, and cybersecurity is not a primary concern and is considered a non-challenge in the smart city field. The next section will discuss the various reasons for the lack of focus for cybersecurity in the category of factors; organizational and financial knowledge and awareness and outsourcing. The reasons for these categories were that there were identifiable common themes in all the literature that had reasonable effects on the consideration of cybersecurity. The category of knowledge and awareness relates to a more personal level, the perception of individuals as it is difficult to measure the knowledge and awareness of an entire organization. The organizational category is then used to capture non-personal factors and relates to organizational decisions, structure and strategy. The financial category includes factors related to more economical factors in nature which can lead to a lack of decisions about cybersecurity. Finally, the outsourcing guide highlights the various factors associated with suppliers and contractors.

Knowledge and awareness: First, there is a need for awareness and knowledge of the potential lack of

cybersecurity in order to impose appropriate constraints. Building a smart city also includes building the foundation for future systems and integration. It describes that a smart city is built to improve the quality of life for citizens and that the infrastructure within smart cities needs the highest level of security in order to secure smart city goals[16]. Moreover, Wenge, etc., describing cybersecurity as a key factor for a successful smart city project. Townsend describes that the digital basis for smart cities will fail, it is a matter of time and extent of the damage it will cause. Thus, smart city infrastructure needs to include security as a priority feature from the beginning, which requires knowledge of smart cities and a long-term perspective.

Smart cities evolve from innovative technology solutions that create additional security threats and challenges. Accessibility and high cost of security applications, data privacy and threats from hackers, viruses, worms and Trojans are some of the challenges of smart cities. Smart cities are mostly unprotected and thus are the target of cyberattacks. Lack of cybersecurity testing, lack of hardware security features and poor security implementation.

Old features and encryption are some of the reasons for successful cyberattacks. The Internet of Things devices on which a large amount of smart city initiatives are built, face particular challenges in the areas of security, standardization, scalability, operability and reliability are factors to consider. Pearce Anderson explains the fact that the people interviewed did not find cybersecurity as a problem that was highly solved. This paper argues that another reason for the lack of focus on cybersecurity, similar to what Pierce and Anderson found is that organizations recognize cybersecurity in smart cities as a challenge.

Hugh etc. describes that there are challenges related to device interoperability which requires common protocol and data formats. However, when systems are built, they need scalability which requires planning for future implementations and agreeing to good performance standards. Gools etc. also note that there is a lack of awareness of mutual dependency on infrastructures as well as weaknesses. Therefore, interoperability is considered a challenge for smart cities and infrastructure failure puts citizens at risk and therefore systems management is of the utmost importance.

Singh etc. describes that information security risks must be identified, compared and categorized according to the severity of the risks in order to explore how the various risks are applied. In order to identify these risks, Chabinsky proposes risk analysis to divide the problem into smaller components. The author argues that anyone involved in some kind of cybersecurity strategy, law, policy or research should complete what are called cybersecurity vectors and the risk framework. First, the organization needs to explore how the organization can prevent an accident at all This could include law enforcement, diplomatic or intelligence efforts. The organization can also focus on reducing vulnerability through more robust security practices, education or security design. Finally, action must be taken to reduce the damage that occurs when a system is compromised.

Future studies: Artificial intelligence is an essential part of the future development of cybersecurity. However, this technology is a double-edged sword: while security experts use developments in the field to identify and respond to threats more quickly, she says, hackers use the same technology to find vulnerabilities.

In smart cities, the scale of turmoil is enormous. Hackers can control the artificial intelligence that controls vital infrastructure, for example, putting water or electricity supplies into the hands of malicious actors. By 2050, we believe hackers will instead have to exploit a series of system vulnerabilities. This means that the technical attacks will be limited to only the best hackers such as the Israeli spy company NSO Group which just said it has discovered how to hack iPhones. “It will be difficult to find real technical weaknesses,” he says.

More optimism about improved security methods: smart phones, for example, already use biometric authentication like fingerprint or face recognition instead of passwords. Since you have things like facial recognition, it becomes silly to have dozens. Of passwords that are managed in very unsafe ways.

This shift is necessary, because despite the difficulty in exploiting technical vulnerabilities in the future, humans are indeed the weakest link in cybersecurity, where the most intelligent individuals in technology are increasingly vulnerable to personal and sophisticated attacks. Therefore, we expect that future studies will be to solve vulnerabilities in cybersecurity. And find solutions to prevent hackers from penetrating the security of smart cities.

CONCLUSION

As smart cities evolve, new innovative technology solutions create additional security threats and challenges. Chourabi etc. identifies the high cost of security, accessibility, data privacy, viruses, worms, threats from hackers and Trojans as some of the challenges of smart cities. These should be considered when building smart cities because they include building the foundation for future systems. In order to improve the quality of life for its citizens, cities need the highest level of security because it is only a matter of time before the digital foundation of smart cities fails. Thus, smart cities require proactive cybersecurity while Johnston and Hill describe that organizations tend to use an interactive cybersecurity approach[14].

McFadzean, etc., describe that the common reason for not focusing on cybersecurity depends on senior manager's awareness of the risks. Therefore, respondent's awareness of the current and future risks of smart cities may be useful to explain the factors contributing to a lack of focus on cybersecurity. In the experimental results, three respondents acknowledged that the future carries threats to smart cities but at present there are no real threats. Consequently, current risk perceptions are generally low which may explain why cybersecurity has not been prioritized. Although the current threat may not be seen as a high priority, smart city initiatives require consideration of future systems to be built or communicated with implementing systems that are not recognized by these experimental results. Therefore, respondent's statements contradict the proactive approach to building a secure foundation, Heo etc, Bartoli etc. suggest. Moreover, IP3 described that there is no comprehensive difference between pre- and post-smart city initiatives. The only real difference is the amount of data. Moreover, the participants do not seem to have recognized the fact that they are building the foundations of the smart city Hugh etc, Bartoli etc. describe smart city initiatives but rather as any other city project. Consequently, respondents do not seem to view smart city initiatives as a comprehensive change for the city which could explain the lack of a long-term perspective[11].

Of the specific risks for smart cities, respondents really focused only on privacy issues with smart cities rather than the high cost of security applications, threats from hackers, viruses, worms and Trojans identified by Chourabi etc. These interviews were conducted at the same time as European Union regulations on data protection and privacy which could distort considerations. However, if these risks are not addressed, there is a high probability of unprotected smart cities which Khatun and Zaidali describe as highly valuable targets of cyberattacks. Smart Cities need to test their cybersecurity, devices, features and encodings to be able to resist cyberattacks[8].

REFERENCES

01. Soceanu, A., M. Vasylenko and A. Gradinaru, 2017. Improving cybersecurity skills using network security virtual labs. Proceedings of the International MultiConference on Engineers and Computer Scientists 2017 Vol II, March 15-17, 2017, IAENG, Hong Kong, pp: 1-6.
02. Japkowicz, N. and Y. Elovici, 2018. Introduction to the special issue on data mining for cybersecurity. IEEE. Intell. Syst., 33: 3-4.
03. Zaffarano, K., J. Taylor and S. Hamilton, 2019. Assessing effectiveness of cybersecurity technologies. Patent and Trademark Office, USA.
04. Zaffarano, K., J. Taylor and S. Hamilton, 2020. Assessing effectiveness of cybersecurity technologies. Patent and Trademark Office, USA.
05. Grossman, R.L., J.E. Heath, R.D. Richardson and K.B. Alexander, 2016. Cybersecurity system. Patent and Trademark Office, USA.
06. Eliot, N., D. Kendall and M. Brockway, 2018. A flexible laboratory environment supporting honeypot deployment for teaching real-world cybersecurity skills. IEEE. Access, 6: 34884-34895.
07. Ni, Z., Q. Li and G. Liu, 2018. Game-model-based network security risk control. Computer, 51: 28-38.
08. Ganesan, R., A. Shah, S. Jajodia and H. Cam, 2017. A Novel Metric for Measuring Operational Effectiveness of a Cybersecurity Operations Center. In: Network Security Metrics, Wang, L., S. Jajodia and A. Singhal (Eds.). Springer, Cham, Switzerland, pp: 177-207.
09. Zhang, R., C. Xu and M. Xie, 2019. Powering hands-on cybersecurity practices with cloud computing. Proceedings of the 2019 IEEE 27th International Conference on Network Protocols (ICNP), October 8-10, 2019, IEEE, Chicago, Illinois, pp: 1-2.
10. Gardikis, G., K. Tzoulas, K. Tripolitis, A. Bartzas and S. Costicoglou et al., 2017. SHIELD: A novel NFV-based cybersecurity framework. Proceedings of the 2017 IEEE Conference on Network Softwarization (NetSoft), July 3-7, 2017, IEEE, Bologna, Italy, pp: 1-6.
11. Pan, J. and Z. Yang, 2018. Cybersecurity challenges and opportunities in the new edge computing+IoT world. Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, March 2018, ACM, Tempe, Arizona, pp: 29-32.
12. Jillepalli, A.A., D.C. de Leon and F.T. Sheldon, 2018. CERES NetSec: Hands-on network security tutorials. J. Comput. Sci. Coll., 33: 88-96.
13. Gates, T. and R. Hirsch, 2019. Determination of cybersecurity recommendations. Patent and Trademark Office, USA.
14. Garman, J.A., B. Johnson and J.J. McFarland, 2018. Cybersecurity incident detection systems and techniques. Patent and Trademark Office, USA.
15. Ferraz, F.S. and C.A.G. Ferraz, 2014. Smart city security issues: Depicting information security issues in the role of an urban environment. Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, December 8-11, 2014, IEEE, London, UK., pp: 842-847.
16. Bagnall, K., R. Casey and J. Jensen, 2020. Intelligent system for mitigating cybersecurity risk by analyzing domain name system traffic metrics. IFI CLAIMS Patent Services, New Haven, Connecticut.