A Comprehensive Analysis of Cyber Security Protection Approaches for Financial Firms: A Case of Al Rajhi Bank, Saudi Arabia

Mohammed I. Alghamdi
Affiliation: Department of Computer Science, Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia
mialmushilah@bu.edu.sa

Abstract

In the modern internet-connected society, technologies underpin almost every action in society. Although there have been positive effects of technologies in the organization, there have been forensic specialists indicating the issues and challenges with cyber security threats. The real-time conditions provide the capability of the organization in detecting, analyzing, and defending individuals against such threats. In this research project, the focus is on understanding the cyber security threats and the protection approaches to be utilized in safeguarding threats from financial institutions. With the Covid-19 pandemic, most of the financial firms, including Al Rajhi Bank, are utilizing technologies in their operations, and this has exposed them to cyber security threats. From the literature review conducted, the financial firms need to consider cyber security approaches including implementing triple DES, RSA, and blowfish algorithms in improving the security measures of the organizations.

Keywords

Cyber security, DES, RSA, Blowfish, Perimeter defense, Access control mechanisms, accountability, Network

1. Introduction

Most of the organizations now are operating in cyberspace, which has meant that cyber security is an issue in such organizations. There has been research regarding cyber security including the protection of the organization's information and data. Organizations have emphasized the complex technology infrastructure, and this has resulted in cyber problems and the offenders are interested in accessing the data and information of the clients. According to Loukaka & Rahman (2017), cyber-security involves measures undertaken in protecting a network or computer from unauthorized access, which will

DOI: https://doi.org/10.54216/JCIM.090101

Received: June 11, 2021 Accepted: November 01, 2021

compromise the integrity and safety of the stored information. As such, cyber security is concerned with technical interventions in protecting data, identity information, and preventing the possibility of unauthorized access. Although governments have been involved in addressing cyber disruption, cybercrimes, and cyber thefts, there have been heightened security measures that should be undertaken in addressing these security challenges. In financial firms, there have been concerns with the implementation of strategic cyber security tools, and this is critical in minimizing cyber security threats. In this research project, an assessment of the cyber security protection approaches that align with the interest of the organization is assessed.

1.1 Al Rajhi Bank: Overview

Al Rajhi Bank is one of the leading financial institutions in Saudi Arabia, and it has been involved in improving its operations through expanding the services offered to the client. As of 2021, the bank experienced a growth of 44% in its customer base and delivered a net profit of SAR 10,734 million in its third quarter. It indicates that the activities of the organizations are increasing, and this will expose the financial institutions to cyber security issues. Tashkandi (2020) indicated that the financial banks in Saudi Arabia needed to consider the security threat associated with the implementation of complex technologies into the banking system. Launching a cyber security campaign for all the financial institutions indicated the significance of Saudi Arabia implementing strategies in reducing the possibility of cyber threats from hackers. With the increase in the customer's operations and transactions, the financial institutions are at threat from hackers, and this will impact their credibility.

According to O'Connell (2020), the Saudi Arabian Monetary Authority provided the Cyber Security Framework in 2017 to safeguard the financial institutions against sensitive data and ensure that the financial sector regains the highest confidence level from the consumers. In managing risk, the ongoing process considers the management of cyber security measures, and this is critical in realizing the effectiveness of the operations and improving the cyber security controls and the occurrences of key vulnerabilities in the industry (Singh, Pasquier, Bacon, Ko and Eyers, 2016). Having this in place is critical in improving the credibility of the operations and ensuring that the emerging threats are addressed and improves the cyber protection initiatives. For Al Rajhi Bank, consideration should be on implementing cyber security measures especially during the current period of cyber-attacks and hacking.

1.2 Related Work

In understanding the cyber security measures, Jang & Nepal (2014) study outlines the theoretical framework explaining the information system's security initiatives. In the case of planned behavior theory (PBT), it indicates that the behavior of the employees can result to security threats and cyber-attacks of the organization's initiatives. With the advancement in technology, most of the financial institutions rely on information systems in managing data infrastructure and improving the quality of the information being shared (Wurm, Hoang, Arias, Sadeghi and Jin, 2016). As such, in studying the behavior of the employees, it is easier to determine the loopholes in the information system framework undertaken in the

DOI: https://doi.org/10.54216/JCIM.090101

Received: June 11, 2021 Accepted: November 01, 2021

organization. Also, Jang & Nepal (2014) outlines the significance of deterrence theory in which the human behavior is affected by detection of cyber-crimes and addressing such measures with ease. There can be deviant behavior among the employees that can compromise access of data by unauthorized individuals. Changing the scope and views of the individuals regarding the cyber-crimes is essential in improving the credibility of the content and enhancing the security initiatives of the organization.

According to Abomhara & Koien (2017), malware attacks often occurred at a single point of the organization, and the hackers exploited the design of the system and the possibility of causing loss of data. Organizations implemented a defense strategy based on using anti-virus and firewall. Detecting accountability and access control mechanism improves the vulnerability of the information technology infrastructure, and it is critical when implementing these measures and addressing the cyber security needs in society (Kaur & Ramkumar, 2021). As illustrated in the figure 1 below, access and control mechanisms were considered effective in reducing the possibility of cyber threats and security challenges. As such, it was necessary in implementing and evaluating intervention approaches that can improve the credibility of the information shared and reduce the possibility of software being compromised. Malware has evolved, and there are new approaches used by hackers in exploiting any loopholes and flaws in the implemented new technologies. This ensured that the security of the company was improved, and there was minimal access to the company's operations. However, with the changing trends in the security system of the companies, new threats emerge, and companies need to discover new protection approaches against cyber-crimes.

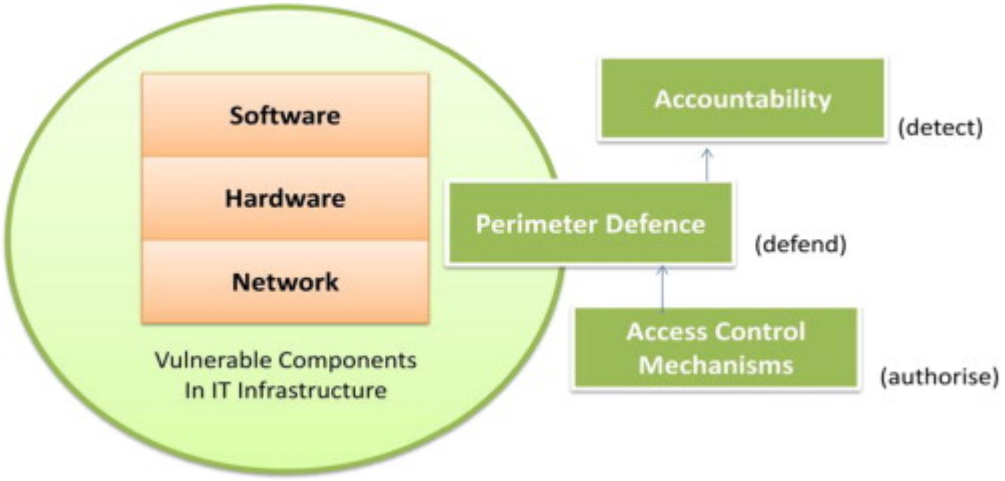

Figure 1: Perimeter defense

Source: Loukaka & Rahman (2017)

Loukaka & Rahman (2017) study indicates that the typical defenses for any organization include installing firewalls to the system and the use of intrusion detection systems. Financial institutions can benefit from the use of the intrusion detection system (IDS) in protecting the organization's internal assets. The main objective of these perimeter defenses is on controlling the incoming traffic and outgoing,

DOI: https://doi.org/10.54216/JCIM.090101

Received: June 11, 2021 Accepted: November 01, 2021

and ensuring that data is analyzed, and determine the network infrastructure towards improving the content delivered. Modern firewall considers network traffic analysis and verification of the IP addresses that are used in accessing the system (Ani, He & Tiwari, 2017). The use of a layered firewall ensures that the network administrators understand the challenges and monitor the operations of the proxy server in determining a harmful application and blocking it. Increasing capabilities and devising measures of sophisticated attackers can easily influence the network traffic and assess the effectiveness of the network layer developed (Ornes, 2016). The importance of the typical defenses is on controlling the data and improving access to the information presented to the organization.

Liang, Biros & Luse's (2016) study explains the significance of using artificial intelligence as a security measure in improving the quality of the content that is shared. The AI programs developed aim at saving resources of the organization as it is not complex, but a constant review of the system should be undertaken in determining defensive measures that the programmers should implement in adjusting to the challenges that are faced the organization, different structure learning techniques have been developed including Neural Structured Learning (NSL) where the interactive databases are used in influencing the trends in the activities (Islam and Aktheruzzaman, 2020). Structured signal helps in improving the data encryption and ensuring that the financial institution experiences an effective platform for reducing the risks as much as possible. Using organized signals in training enables the developers of the system to deliver robust AI models that cannot be compromised with ease and helps organizations in constructing representations that improve the security of their system.

According to Seemma, Nandhini & Sowmiya (2018), the increase in internet use in the different institutions has meant that priority should be on cyber security as this heightens the attention given to improving the efficiency of the system. Information and data collected can be easily accessible in modern society, and the company should regulate the implementation of such initiatives in ensuring that increasing dependence on cyberspace technologies in managing human factor risks (Airehrour, Gutierrez and Ray, 2016). In modern organizations, there are vulnerabilities, especially where the employees are working remotely due to the Covid-19 pandemic. People have been subjected to wide arrays of problems that can affect the security of the system. It is necessary to consider social engineering in gathering information and exploiting any weaknesses in the system, and this should always be assessed and investigated in mitigating the challenges that might affect the organization (Kumar, Tiwari & Zymbler, 2019). When the organization develops and promotes positive security culture, there is the possibility of reducing the chances of the data and information being accessed by third parties. Assessing the environment and determining the possibility of vulnerabilities to the system is critical in reducing the challenges that might be caused by the system being compromised.

Sawyer & Hancock's (2018) study assesses the internet of things (IoT) and the possibility of challenges when the organization implements IoT in its operations. One of the key challenges that can impact the organization is data confidentiality in which the information in the system can be accessed by unauthorized people due to the system being compromised (Sadique. Rahmani & Johannesson, 2018).

DOI: https://doi.org/10.54216/JCIM.090101

Received: June 11, 2021 Accepted: November 01, 2021

As such, it is important to address two main issues-authorization mechanisms and access control. There is also the challenge of identity management mechanism where verification of the authorized person's identification should be a priority before they are allowed to access the system (Malina, Hajny, Fujdiak, and Hosek, 2016). Making access control mechanism is critical in establishing measures in creating and manipulating the identity management, and this is essential for the IoT environment and deciphering measures that entities can stay connected but secure their data (Ahmad, Niazy, Ziar & Khan, 2021; Atamli and Martin, 2014). In most organizations, developing IoT mechanisms should be followed by strong security measures, and this can improve the data encryption and the security of information that is shared among individuals. For the IoT devices, privacy is considered to be an integral component that the management should assess, and data communication should only be between the authorized persons to access the system (Gupta, Tewari, Jain & Agrawal, 2017). With the understanding of the challenges and issues facing the organization, a review of the trend in the operations of the management is critical in improving the security system of the entity in the long run.

According to Simmonds (2018), vulnerabilities in the system are one of the weaknesses that the intruders determine when accessing the system. The use of access control systems, it provides the management with the information on the best measures and strategies to be undertaken in limiting such unauthorized access to the system. One of the key issues includes authentication of the system where there should be verification of the individuals accessing the system. This can be done using the personal identification number or password encrypted to the system. As noted in Stewart & Jürjens (2017), having strong authentication ensures that there is minimal risk of third parties accessing the system. Also, the management should ensure that there is accountability when accessing the system. This involves logging in and out of the system and ensuring that only the authorized individuals are given access to the database. Information on the history of logins and logoffs should always be availed and such files are accessed in preventing the possibility of the employee's giving information to the third party (Lu, 2018). Developing a clear framework in which the information and content can be authenticated is essential for any organization that aims at realizing the credibility of the system and minimizing third-party access to the system.

Interestingly, cyber-attacks have consistently evolved and there should always be new approaches in place to address the vulnerability in the system. Cybercriminals are involved in modifying the malware signatures that exist in the system and ensure that they exploit the new flaws reported in the new technology implemented (Gupta, Tewari, Jain & Agrawal, 2017). Injecting malware into the system is done when the hackers have explored the current system and determined its flaws. There are common attack patterns that can be experienced in society including web browser attacks, non-PC based attacks such as VoIP and tablets. Stewart & Jürjens (2017) study indicates that social media networks have been the haven of activities for most organizations, and the hackers have capitalized on this method in increasing vulnerability of the social media craze. As noted in Senol & Karacuha (2020), most of the organizations and individuals share their information on these social media platforms, and they are

DOI: https://doi.org/10.54216/JCIM.090101

Received: June 11, 2021 Accepted: November 01, 2021

unaware that they are providing vital information to the hackers in which they can use such platforms in accessing other financial information in improving the quality of the contents that is share. Having this in place can create an effective measure that can be integral in achieving the success of the operations. With this in place, the management can be critical in realizing success in the cyber security initiatives towards achieving success in the operations.

2. Methodology

A research methodology used in the empirical analysis for predicting the change in the information security system of the organization is proposed. In developing approaches to cyber security, the risk should be addressed, and this is expressed as a relationship between the vulnerability of the system and the possibility of individual threat occurrence:

$$\text{Risk}_n = f(\text{threat}_{en}, \text{Vulnerability})$$

The first strategy in cyber security management is risk identification, and this starts with a valuation of a firm's assets, implying that there should be a consistent approach in determining qualitative and quantitative values. Some of the factors are costs associated with asset acquisition and data maintenance costs. Secondly, threat analysis where identification of known potential threats, and the probability of such threats occurring in the organization. Thirdly, vulnerability analysis is conducted, and this helps in determining the best approach to be utilized in information security systems.

3. Experimental validation:

An observational method will be utilized for this study in which the analysis will be on the trends in the cyber security frameworks employed by Al-Rahji Bank. Project monitoring will be conducted in determining the vulnerability of the current security measures that are in place in the financial institution. The project will be reviewed for the past five years and determine incidences of security breaches in its system.

Also, case study analysis will be utilized, and the data observed for the past five years. With a comparison of different methods developed by other organizations, appraisal of the cyber security approaches will be determined, and this will improve the decisions on the effective recommendations to be made on the project.

4. Implementation

With the changing trend in the security system of the organization, Al Rajhi Bank needs to implement strong encryption algorithms. The options recommended for the bank include:

4.1 Triple DES

The design of Triple Data Encryption Standard (DES) algorithm was developed to facilitate control of unauthorized access to the organization's data (Sari, Rachmawanto & Haryanto, 2018). The 3-

DOI: https://doi.org/10.54216/JCIM.090101

Received: June 11, 2021 Accepted: November 01, 2021

key encryption was implemented following the hackers making symmetric-key method to be obsolete in securing the organization's data. There were vulnerabilities with the symmetric-key method, and this affected the success of protecting the data from the hackers (Ratnadewi *et al*, 2018**)**. The encryption process follows the encryption of plaintext blocks, as the first initiative, using the single DES and K_1 followed by DES reverse cipher with K_2. A detailed process of data encryption is provided in figure 2 below. This process of securing the system has been widely used, and it has been successful in protecting the companies against vulnerabilities in hacking to their system. The algorithm of DES relies on 64-bit key, and the total bits of 168 can be added to the system. The complexity in which triple DES is encrypted makes it slower and difficult to crack by hackers. As such, for Al Rajhi Bank, can rely on Triple DES encryption for hardware purposes, and this will improve its security measures and the possibility of the hardware being compromised by hackers.

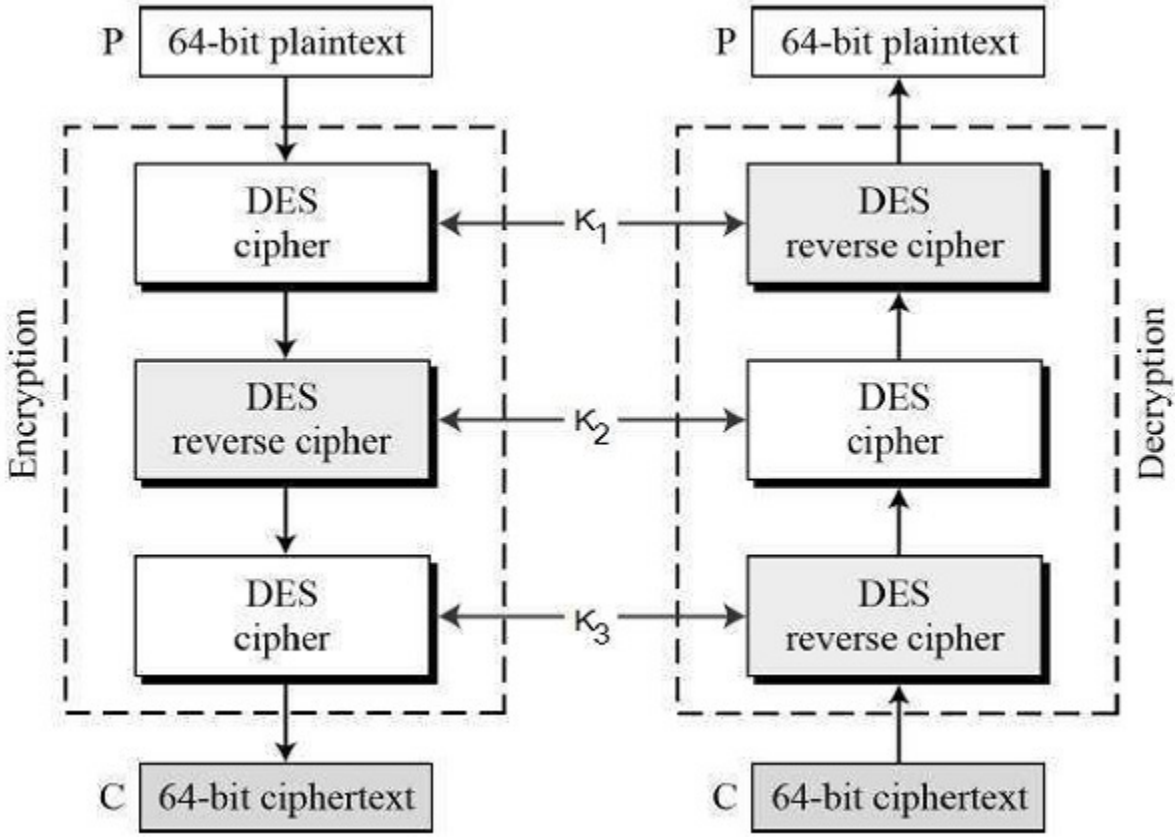

Figure 2: Triple DES

Source: **Sari, Rachmawanto & Haryanto (2018)**

4.2 RSA

Secondly, Al Rajhi Bank can consider the Rivest-Sharmir-Aldeman (RSA) encryption. It is considered to be asymmetric encryption due to the availability of private and public keys. The keys for the development of

DOI: https://doi.org/10.54216/JCIM.090101

Received: June 11, 2021 Accepted: November 01, 2021

the RSA are based on the algorithms of the large numbers, which are critical in securing the system and ensuring that the information cannot be accessed by unauthorized people. RSA algorithm is complex especially when formulating the keys as it requires the use of large numbers. As such, it makes RSA better than DES, and it improves the overall security of the content that is shared in the organization. Using this encryption in the organization is critical in improving the activities and operations of the organization. Improving the information being shared in the organization can be realized through assessing the data credibility and data privacy of the financial institutions.

4.3 Blowfish

With the use of Blowfish encryption, the financial institution can benefit from securing payments that customers make through the use of internet services and managing the passwords. Blowfish is considered to be symmetrical encryption, and this follows the algorithm of breaking data and sending such data in chunks, which is essential in improving the quality of the information being shared (Zammani & Razali, 2016). Patenting the content and information shared is essential for the company, and it is a necessary tool in ensuring that the credibility of the information is assured. Consumers will only be linked to a financial institution that its interest is on safeguarding the needs of the customers. The decryption of this algorithm is faster and it can easily determine the attack and prevent it from harming the system. Financial institutions are faced with the challenge of data being easily accessed where there is no strong encryption on its database system. As such, the financial institution can improve its data security by utilizing the different components of encryption to the benefit of the entity.

5. Conclusion

The implementation of cyber security measures is critical in realizing the success of the operations, and this is essential in achieving a competitive edge in the industry. The dynamic nature of the operations has meant that cyber security is a priority, and there is a need for protection approaches to be undertaken as a way of enhancing the privacy and confidentiality of customer's data for the Al Rajhi Bank. Developing a mechanism in which the securitization of the cyber security initiatives for the organization has always been the voice of the Saudi Arabian Monetary Authority on the implementing of the Cyber Security Framework model. Focusing on the changing trends in the economy and the changes in the hackers approach to attacking the system should be the foundation for implementing a secure system for the organization. Al Rajhi Bank can utilize the Triple DES encryption for its hardware protection, RSA, and Blowfish as a way of reducing vulnerability to the bank’s database. In understanding the challenges faced in the organization, the management can improve the credibility of its activities and improve the overall cyber protection initiatives

DOI: https://doi.org/10.54216/JCIM.090101

Received: June 11, 2021 Accepted: November 01, 2021

6. Future Work

With the changing trends in cyber security measures, there have been emerging trends in the cyber security measures. As such, researchers should consistently review the changes in the cyber security measures, and implement new encryption keys in securing the data of such organizations. Future work can also be directed to financial institutions in less developing economies and understand challenges they face when they are not using sophisticated cyber security approaches in their systems.

References

[1] Abomhara, M. & Koien, G. (2017). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders, and attacks. Journal of Cyber Security, 4(12), 65-88

[2] Ahmad, I., Niazy, M., Ziar, R. & Khan, S. (2021). Survey of IoT: Security threats and applications, Journal of Robotics and Control, 2(1), 42-47. DOI: 10.18196/jrc.2150

[3] Airehrour, D., Gutierrez, J., and Ray, S. K. (2016). Secure routing for internet of things: A survey, Journal of Network and Computer Applications 66, 198–213.

[4] Al Rajhi Bank. https://www.alrajhibank.com.sa/en/alrajhi-group/media-center/press-releases/al-rajhi-bank-delivers-sar-10734-million-in-net-profit-for-the-first-nine-months-of-2021

[5] Ani, U., He, H. & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. Journal of Cyber Security Technology, 1(1), 32-74. https://doi.org/10.1080/23742917.2016.1252211

[6] Atamli, A. W., and Martin, A. (2014). Threat-Based Security Analysis for the Internet of Things, International Workshop on Secure Internet of Things, 35–43

[7] Burton, J. & Lain, C. (2020). Desecuritising cyber security: Towards a societal approach. Journal of Cyber Policy, 5(3), 449-470. https://doi.org/10.1080/23738871.2020.1856903.

[8] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: State of the art and future challenges. Neural Computing and Applications, 28(12), 3629-3654.

[9] Islam, M. and Aktheruzzaman, K. (2020) An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions. Journal of Computer and Communications, 12(8), 11-25. doi: 10.4236/jcc.2020.84002

[10] Jang, N. & Nepal, S. (2014). A survey of emerging threats in cyber security. Journal of Computer and System Sciences, 80(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

[11] Kaur, J. & Ramkumar, K. (2021). The recent trends in cyber security: A review. Journal of King Saud University-Computer and Information Sciences, 12(9), 21-27. https://doi.org/10.1016/j.jksuci.2021.01.018

[12] Kumar, S., Tiwari, P. & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6(2), 111-126. https://doi.org/10.1186/s40537-019-0268-2

[13] Liang, N., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. Journal of Management Information Systems, 33(2), 361-392.

[14] Loukaka, A. & Rahman, S. (2017) Discovering new cyber protection approaches from security professional prospective. International Journal of Computer Networks & Communications, 9(4), 13 -24. DOI: 10.5121/ijcnc.2017.9402

DOI: https://doi.org/10.54216/JCIM.090101

Received: June 11, 2021 Accepted: November 01, 2021

[15] Lu, Y. (2018). Cybersecurity research: A review of current research topics. Journal of Industrial Integration and Management, 3(4), 21-31. https://doi.org/10.1142/S2424862218500148.

[16] Malina, L., Hajny, J., Fujdiak, R., and Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. Computer Networks, 102, 83–95.

[17] O'Connell, N. (2020). Cyber security in the Saudi financial services sector: The SAMA cyber security framework. https://www.tamimi.com/law-update-articles/cyber-security-in-the-saudi-financial-services-sector-the-sama-cyber-security-framework/

[18] Ornes, S. (2016). Core Concept: The Internet of Things and the explosion of interconnectivity, Proceedings of the National Academy of Sciences, 113(40), 11059–11060.

[19] Ratnadewi *et al* (2018). Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC). Journal of Physics: Conference Series, 14(8). 1-19. doi :10.1088/1742-6596/954/1/012009.

[20] Renaud, K., Orgeron, C., Warkentin, M. & French, E. (2020). Cyber security responsibilization: An evaluation of the intervention approaches adopted by the five eyes countries and China. Public Administration Review, 2(1), 12-24

[21] Sadique. K., Rahmani, R. & Johannesson, P. (2018). Towards security on internet of things: applications and challenges in technology. Procedia Computer Science, 141(8), 199-206. https://doi.org/10.1016/j.procs.2018.10.168

[22] Sari, C., Rachmawanto, E. & Haryanto, C. (2018). Cryptography Triple Data encryption standard (3DES) for digital image security. Scientific Journal of Informatics, 5(2), 12-21

[23] Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. Human Factors, 60(5), 597-609

[24] Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), 125-128

[25] Senol, M. & Karacuha, E. (2020). Creating and Implementing an Effective and Deterrent National Cyber Security Strategy, Journal of Engineering, 12(4), 1-19. https://doi.org/10.1155/2020/5267564

[26] Simmonds, M. (2018). Instilling a culture of data security throughout the organisation. Network Security, 2018(6), 9-12.

[27] Singh, J., Pasquier, T., Bacon, J., Ko, H., and Eyers, D. (2016). Twenty Security Considerations for Cloud-Supported Internet of Things, IEEE Internet of Things Journal, 3(3), 269–284.

[28] Stewart, H., & Jürjens J. (2017). Information security management and the human aspect in organizations. Information and Computer Security 25(5), 494–534.

[29] Tashkandi, H. (2020). Online mask ads mystery revealed as Saudi banks launch cybersecurity campaign. Arab News. Retrieved from https://www.arabnews.com/node/1767466/saudi-arabia

[30] Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R., and Jin, Y. (2016). Security analysis on consumer and industrial IoT devices, 21st Asia and South Pacific Design Automation Conference (ASP-DAC), IEEE, 519–524.

[31] Zammani, M., & Razali, R. (2016). An empirical study of information security management success factors, International Journal of Advanced Science, Engineering and Information Technology, 6(6), 904-913.

DOI: https://doi.org/10.54216/JCIM.090101

Received: June 11, 2021 Accepted: November 01, 2021