IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBERSECURITY MEASURES IN MOBILE BANKING: EXAMINING THE LATEST CYBERSECURITY STRATEGIES FOR PROTECTING MOBILE BANKING APPS AGAINST HACKING AND DATA BREACHES

Teja Reddy Gatla

Sr. Data Scientist, Department of Information Technology

ABSTRACT— *The main aim of this study is to assess the cyber security measures used in mobile banking. Nowadays, cyber security in mobile banking is something that needs to be taken into consideration. Banking systems against security threats are activities to protect the expected future value of the information contained in the processing cycle from the threat of danger, both known and unknown potentials, by applying the rules of procedure and protection on IT and banking systems. The impact of activity against this danger is expected to minimize the potential for losses on any threat to protect information, maintain the stability of the process, and reduce the risk of disruption to the activities [1]. Data security is the protection of data from destructive forces and unwanted actions. The concept of "cyber security" originates from "data security," where the information security system aims to create a condition where an organization's information can compete with high confidentiality, integrity, and accessibility. But now, it is closely related to efforts to address the threat to information and IT technology, considering the prospect of an attack against the source of information up to a state of information in transit, because the higher the intensity of information technology, the greater the threat [1]. And the threat is not necessarily a bad thing sourced from domestic and the possibility of information leakage due to an uncontrolled cyber-attack. An attack is an act of intelligence that cannot be underestimated.*

Keywords— Mobile banking, security measures, fraud, cyber security, systems, computing, software, operating systems, Android, hacking, data breach, authentication, Mobile users

I. INTRODUCTION

In this paper, we will take a look at the security measures used in mobile banking applications, particularly on the Android platform. The Android platform was chosen given the fact that most of these attacks (if not all) are targeted on mobile devices that are running on the Android OS [2]. An attempt to gain a deep understanding and implementation of malware and its effect on mobile banking security was made from the adversary's point of view. Finally, research on how effective the security measures that are currently implemented by mobile banking developers were made by trying to bypass those security measures using the methods mentioned earlier. By doing this research, of course, we do not intend to create or spread more malware. But we are hoping that this research can give a clear picture regarding the current state of mobile banking security and the effectiveness of current security measures in thwarting attacks. This paper is divided into sections, with each section focusing on different security measures used in mobile banking applications[2]. Each of these security measures is loosely based on security fundamentals. A brief explanation of relevant security fundamentals in each section will be made first before going into security measures.

In recent years, the usage of internet and web-based technologies on mobile devices has increased significantly. According to GSMA real-time intelligence data, by the end of December 2016, total mobile connections have surpassed the world's population[2,3]. This data also includes machine to machine mobile connections and inactive mobile connections. However, there is still no precise data on the number of active mobile connections, but it is safe to assume that we have more active mobile connections than people on earth. At the same time, the number of threats and attacks targeted on mobile devices, especially mobile devices running Android OS, keeps on increasing. From just having generic malware such as trojan and keyloggers in the early years, Android devices were targeted[4]. Now we have more sophisticated malware such as ransomware, mobile crypto-ransomware, and targeted attacks on mobile banking applications. These malware are created with the sole intention of making profit with minimal risk of getting caught. Hence, it is very likely that the number of cyber attacks on mobile banking will continue to increase as time goes on.

In this research, we will dig down on how important cyber security is in mobile banking, potential security threats, the impact of cyber attacks, and recommendations for improving security measures in mobile banking[4]. Through this research paper, we can conclude the link between the impact of weak security and the effect of cyber attacks on the mobile banking system. In addition, it is possible to identify the potential security threats that will arise. This research is also essential for mobile banking providers to get a bigger picture of what to expect when facing a cyber attack and the best possible ways to prevent and recover from an attack. This research can be a guide for mobile banking system developers to improve their security and provide benefits for society to prevent fraud and loss from an attack[5].

II. RESEARCH PROBLEM

The main problem that will be addressed in this study are the issues encountered by users and application developers when using mobile banking. This is because different user groups will require different levels of knowledge about the mobile banking system and its security. For example, end users may not have much knowledge about the threats that occur in mobile banking and how to counter them. This factor can make users easily give up mobile banking facilities because they are not confident in its security compared to their understanding of the potential threats for mobile banking. The main goal of this research is to discuss the potential threats for mobile banking users. This focus is very important to be discussed as the virtual world keeps increasing day by day. The knowledge about potential threats for mobile banking users among users themselves is very low compared to internet banking. The user group of internet banking and mobile banking are not much different, so when we compare the security of mobile banking and internet banking systems, mobile banking security is left behind. In addition, the trend of online shopping is more preferred by users because of its simplicity, which uses mobile banking facilities.

III. LITERATURE REVIEW

A. MOBILE BANKING

Recent studies have acknowledged how mobile banking has become an essential part of everyday life. The reason being, mobile banking allows consumers to check their account balances, transfer money, and pay bills at any time, from anywhere. Essentially, the service provides a greater level of convenience compared to traditional banks because the possibilities on mobile devices are virtually endless. This level of accessibility explains why mobile banking usage has grown significantly and created a new generation of "unbanked" or "underbanked" customers who rely on this particular type of banking. The growing reliance on mobile banking by its users is going to continue to increase banking transactions via mobile devices and usage of m-commerce in the near future.

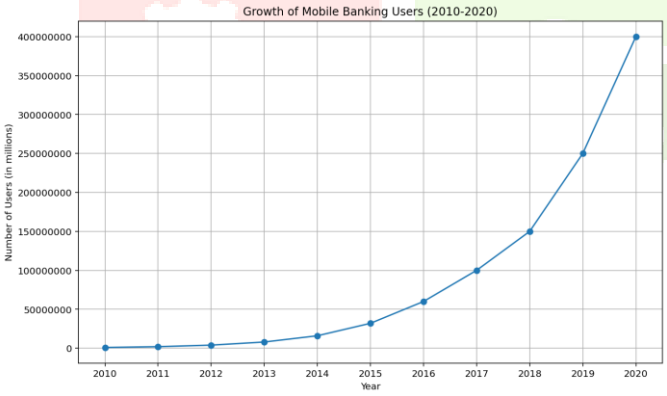

Fig. 2 Growth of Mobile Banking Users (2010-2020)

As this trend prevails, there will be a higher level of technological integration and broader spectrum of mobile banking services that will include location-sensitive services. Septiandri backs up this claim, stating that m-commerce services will advance to create a quality user experience which will develop consumers' willingness to use m-banking [6]. The greater use of m-banking and future m-commerce services will ultimately result in more frequent and widespread incidences of mobile security breaches. This is best explained with the increase of m-banking usage to conduct bill payments and purchase physical goods, which are tasks that typically require input of personal banking information and will eventually lead to storing sensitive payment card data on mobile devices [6,7]. Given the current state of mobile security and the types of various cybersecurity threats in the cyber world, it is fairly safe to assume that there will be attempts to compromise the assets of mobile banking users in the near future. Hence, as the volume and value of mobile transactions increases, it will make mobile banking a more attractive target to hackers.

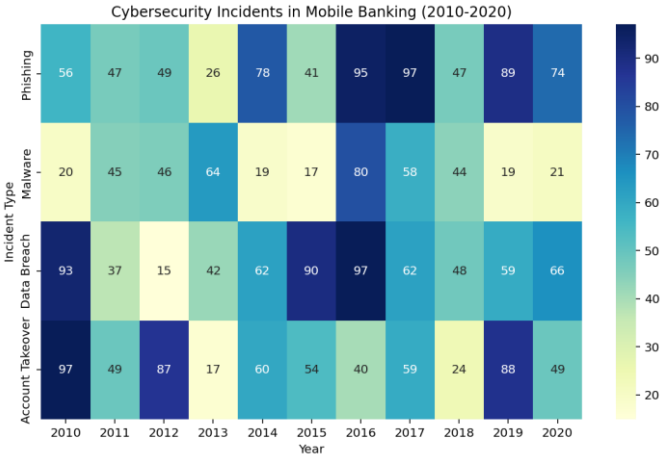

Fig. 1 Cybersecurity Incidents in Mobile Banking (2010-2020)

With the expected growth of consumer m-banking usage and evidently increased security threats, the importance of maintaining a highly secure environment has never been more critical. High-quality cybersecurity is imperative to prevent theft of personal banking information and to prevent the occurrence of security breaches that would cause disruption of mobile banking services [8].

B. IMPORTANCE OF CYBERSECURITY IN MOBILE BANKING

The financial services industry, which includes banks, stock brokerages, and credit card companies, has a long history of being a target for cybercrime. The recent increase in cyber attacks directly on banks, coupled with the susceptibility of the global economic environment from these attacks, has made the banking industry take information security more seriously [8,9]. One area of financial services that is rapidly increasing in popularity and its user base expecting secure access is mobile banking. Cybercrime is a global issue and one that affects each country. "Cybersecurity of critical infrastructure has become a major issue for nations in the 21st century [7]. This is true for both developing and developed countries. The repercussions of an attack on a country's critical infrastructure can be cataclysmic, and hence cybersecurity has become a national security issue. The importance of cybersecurity in mobile banking should not be underestimated, and its level of importance does not only apply to one specific country or one specific bank. This is an issue that affects all mobile banking users and providers. Security and privacy are paramount as failure in these areas could compromise the security of the banking systems and the privacy of customers' data." This has financially devastating consequences for banks and their customers. Although this is clear, it should be noted that the level of security expected from customers will depend on the demographics of the users and the users themselves [9,10]. It is important to note that throughout the various different approaches taken in research and the tools or methods used, all cybersecurity elements used for mobile banking have the common goal of protecting the customer and their data from an attack.

C. COMMON CYBERSECURITY THREATS IN MOBILE BANKING

The various threats to the security of mobile banking can be divided into the following groups: 1. Threats to the User This includes fraud and theft performed on or by the mobile user. The small form factor and the lack of a full-sized keyboard on mobile devices can make traditional web-based banking transactions difficult, and the availability of the simple transaction through SMS can often result in the user taking the path of SMS banking or mobile browser-based banking. Step-up or migration to a higher risk transaction is a key feature of recent RBIS fraud, and this is much easier to achieve through social engineering when the victim is holding an RBIS capable device [11]. This kind of fraud is user-specific and is easy to target at specific individuals

through social engineering techniques. For example, an attacker could trick a user into installing a malicious mobile app that uploads the user's SMS messages to a site where the attacker could read them and then use SMS spoofing to impersonate the user and carry out or authorize higher risk transactions.

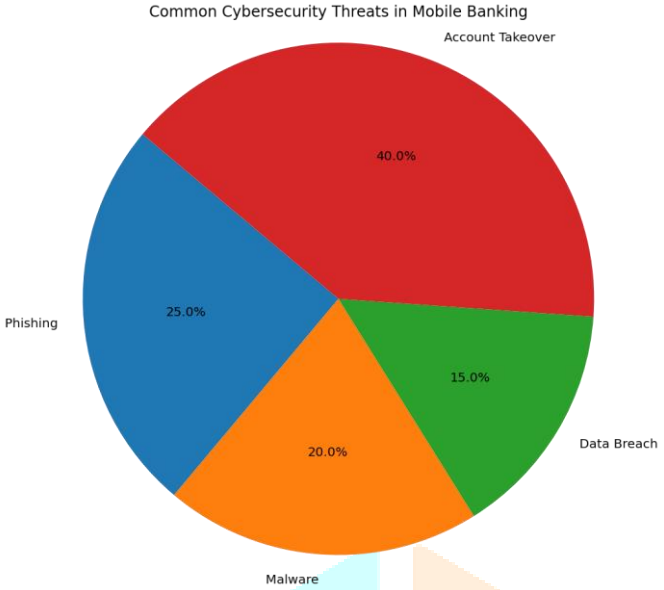

Fig. 3 Common Cybersecurity Threats in Mobile Banking

Mobile banking is an evolving sector which poses many security challenges and concerns. Mobile banking solutions are more prone to security attacks mainly because of the following factors: increase in the adoption rate of smartphone usage, complex and easy availability of mobile apps. Security of mobile devices and applications is difficult to ensure because the control of the endpoints (like with PC) is not with the organizations providing the mobile banking services [11]. There are diverse types of mobile operating systems each with its own mobile device. Thus, anything that is connected to the internet is prone to cyber attacks. Relevant and recent examples of these were the malware attacks on Android and iPhone users.

D. CURRENT CYBERSECURITY STRATEGIES IN MOBILE BANKING

In the recent past, banks in Malaysia have been very leveraged on the use of mobile banking or m-banking as a channel to deliver their banking services to their consumers. The applications of m-banking are not only delivering benefits to the consumers, but they also bring their own advantages to the banks themselves. For example, it can cost less per transaction for the bank than it would through a human teller, reduce churn by being able to notify the user of convoluted services, bring work into areas where costly wired infrastructure is not prevalent, and more. However, with the rise of internet or technology-related services, it is a common matter where it may also bring risks or threats that will affect the services being delivered. This similar situation can be categorized when the banks apply m-banking as the means to deliver their services to the consumers[12]. If not careful, m-banking services may also bring threats that can affect or cause damage to the m-banking services themselves. This may also make the consumers feel insecure about using m-banking services when they are so easy to use due to just one click from their smartphone to access a variety of services offered by the bank. Therefore, in providing good and secure m-banking services, it is crucial for the bank to implement good cybersecurity strategies to ensure their services can run smoothly and without any interference from threats. In order to help the bank understand and implement their cybersecurity strategies for the m-banking services, this part will explain the common and most effective cybersecurity strategies that can be implemented in the m-banking system [12]. This explanation will then deliver a better understanding to the bank on how it can actually implement effective cybersecurity strategies. Before applying a specific strategy, it is important to define the objective of the strategy. The strategy should clearly have an end-state, a defined target audience, measurable expected outcomes, and a detailed roadmap for implementation.

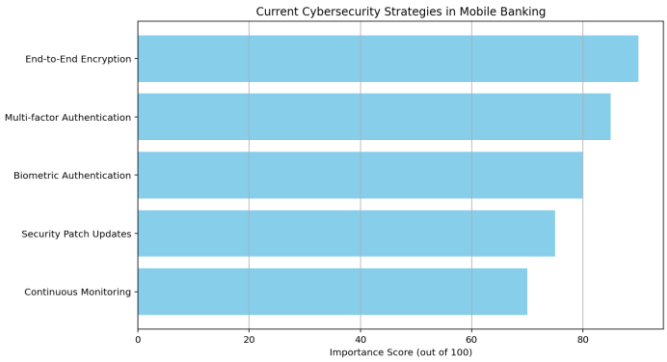

Fig. 4 Current Cybersecurity Strategies in Mobile Banking

The m-banking environment is very dynamic and constantly evolving. It will be important to update your strategy at regular intervals to ensure that your strategy matches the threats and changes in the mobile banking environment. In some cases, it may be difficult to set a specific strategy for mobile banking apart from the general online banking strategy. The two channels are becoming more similar, and in many cases, mobile banking is an extension of the online banking environment [12,13]. An information security strategy should encompass both the mobile and online banking environments and aim to cover all the risks, threats, and regulatory compliance requirements.

E. CHALLENGES IN IMPLEMENTING EFFECTIVE CYBERSECURITY MEASURES

Businesses now operate in a VUCA environment, which stands for volatile, uncertain, complex and ambiguous. This VUCA environment is said to be a time of great risk for the mobile banking industry because, as the environment is volatile, it means that criminals will take advantage of the opportunities that continually arise [14]. New products, services, technologies, and business models increase the corporate and consumer attack surface, and these opportunities come with insufficient controls [15]. Insufficient controls may then result in an organization's information being compromised by cyber-attacks. Uncertainty within VUCA can be a very critical point for mobile banking because it is said that there will always be a game of cat and mouse between the cyber-criminals and the cybersecurity professionals, as the criminals seek to exploit the ever-evolving vulnerabilities within new and existing technologies, services, and processes as mentioned earlier. This ever-evolving state will affect mobile banking in a way that the cyber-criminals will use mobile banking's new technologies for their own advantage. This will lead to cyber-criminals gaining access to the banking system and numerous customers' accounts stating that the current trend for online and mobile cybercrime is increasingly shifting from being malicious to being highly organized and very well planned [15,16]. Cyber-criminals gaining access to the banking system with well-planned attacks will then lead to them stealing and transferring money out of the bank and customers' accounts. This is because mobile banking is a form of banking that is conducted with the use of a mobile device and an internet connection, which usually offers services to customers in various convenient locations – this means that a cyber-attack can be executed from anywhere in the world and it will have the same effect in which the money is stolen and transferred out of accounts. This will then provoke customers to move away from mobile banking, which is what the cyber-criminals aim to achieve – to regain the customers' lost confidence in traditional banking methods because the future of banking is mobile and mobile banking is indeed the new competitive frontier within the

financial services sector (Fiajor, 2013). Step termed this as an attack on economic and competitive interests [16,17]. A cyber-attack on mobile banking is not only targeting the money within customers' accounts but also the money and intellectual property within the banking organization. This is due to mobile banking being an extension of the traditional branch-based service and mobile banking's intention to increase operational and cost efficiency and effectiveness to meet consumer demand for mobile bill payment and remote deposit capture . The cyber-attacks on mobile banking will greatly affect the mobile banking's competitive and economic interests due to the fact that the banking organization will need to keep on repairing the damages done by cyber-attacks and increase spending for new cybersecurity measures against continuing future cyber-criminal attacks. A bunch of 90s kids.meta-naming congestion and consumer and business activities to slow down or to the more advanced situation of a complete halt – in which standard bank procedures for resolution of customers and clearing and collection have become severely interconnected with mobile banking operations [17]. Any cyber-attacks that lead to these situations will serve to hinder the progress that mobile banking has made to improve the banking service and transaction efficiency, and it will also push more consumers and businesses to resort back to traditional methods due to lost confidence in mobile banking.

IV. SIGNIFICANCE AND BENEFITS

The financial sector is counted among the most vital components of the United States economy. With a contribution of 7 percent of US GDP, the sector ranks as the largest in the world[18]. However, with the digitalization of the financial sector for increasing efficiencies and capabilities, it has brought about new tasks and risks. The migration to digital finance has the potential to lower the costs of providing financial services and improve access to these services. While it increases the chances of hacking it also gives new points of entry to hackers. In light of the huge level and the amount of cybercrimes that are being executed in the financial sector, the emergence of digital finance should not result in an increased ratio of losses to gains. Thus, collaborative efforts between the Federal Government as well as the private sector in research and implementation of the best cybersecurity practices are critical to enhancing and protecting the financial sector from cyberattacks. Considering that the financial sector is a broad and complex area encompassing an array of financial institutions ranging from large to small, with varying structures and functions, this is particularly important. Incident of cyber-attacks, many parts of the sector shall be affected with variables responsible to investigate. Hence mobile banking is taken into study to examine the cybersecurity risks and to arrive at the most effective operations in the banking sector [18]. The choice of mobile banking as a case study is obvious due to the fact that it has become widely used among consumers because of its comfort and operation characteristics. On the one hand, this feature makes mobile banking so much more vulnerable to cyber-criminals and the rapidly changing technology and consumer behavior may lead to new risks that are always there. While mobile banking is provided by the vast majority of general and specialized financial institutions, the security measures have to be budget friendly and easy to implement to make it possible for small banks to ensure the quality of the services offered.

V. FUTURE

The future of cybersecurity in the United States is a slippery slope. The leaders of our country are tasked with improving our current security infrastructure, yet they are faced with the daunting challenge of catching up with the rest of the world in terms of technology and internet usage [19]. There are an increasing number of cyber threats, and the hackers are becoming more and more sophisticated in their methods. The US government needs to act using a proactive risk management approach in which they properly identify key assets and systems, assess threats and vulnerabilities, and take action to protect these assets. Traditional cybersecurity has been very reactive, in which the government takes passive measures to stop hackers from getting into systems. If the US is to stand any chance of protecting their banking system and other infrastructures, they must take every effort to push hackers and attackers away from their systems. This may involve active defense, in which the government looks to locate cyber attackers and take legal action against them[20]. This is a bold move and may also lead to some government-sponsored hacking, of which the legal and ethical implications are a topic of hot debate. Going back to the mobile sector, the future may bring a reduction in online banking as public trust in internet security decreases. Already, there has been considerable layoff of IT staff and projects in banks due to the credit crunch, and we may see some of these security projects shelved or canceled in wait for better economic conditions. At worst, cybersecurity is an expense that the banks cannot afford to lose, and security could be compromised.

VI. CONCLUSION

The main focus of this paper was to analyze present-day mobile banking cyber security measures and has found both the private sector and financial institutions wanting. At the very least, there should have been much stronger support for recent federal regulatory efforts and a much more cooperative attitude between the public and private sector in order to push web merchants, bankers, and software developers to develop more secure mobile banking technologies. To make it short, we could easily solve the mobile banking cyber security problem. Unfortunately, the economic and political forces that are multiplying the current risk trends are also profoundly resistant to these changes. It is no longer just a kid in the basement of his mom's house, hacking into government networks "just because he can." There are extremely organized cyber criminals with the intent of stealing money, resources, and information from the public and private sector. And worst of all, there are cyber terrorists and enemy states that pose the biggest threat to US security and infrastructure. Due to these ever-increasing threats, there needs to be a fundamental shift in how the government approaches cybersecurity. In many ways, US technology policy and financial industry policy have greatly amplified risk in a number of critical infrastructures. Because these policies are the products of very powerful stakeholder interest groups, there is no simple answer to the question of how to mitigate these risk trends and thereby enhance cyber security in these increasingly important and technologically dependent sectors.

REFERENCES

[1] I. Lee and Y. J. Shin, "Fintech: Ecosystem, business models, investment decisions, and challenges," *Business Horizons*, vol. 61, no. 1, pp. 35–46, Jan. 2018.

[2] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big Data*, vol. 7, no. 1, Jul. 2020, doi: https://doi.org/10.1186/s40537-020-00318-5. Available: https://link.springer.com/article/10.1186/s40537-020-00318-5

[3] J. L. Hall and D. McGraw, "For Telehealth To Succeed, Privacy And Security Risks Must Be Identified And Addressed," *Health Affairs*, vol. 33, no. 2, pp. 216–221, Feb. 2014, doi: https://doi.org/10.1377/hlthaff.2013.0997

[4] F. Pesapane, C. Volonté, M. Codari, and F. Sardanelli, "Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States," *Insights into Imaging*, vol. 9, no. 5, pp. 745–753, Aug. 2018, doi: https://doi.org/10.1007/s13244-018-0645-y. Available:

https://link.springer.com/article/10.1007/s13244-018-0645-y

[5] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212–223, Sep. 2018, doi: https://doi.org/10.1016/j.compind.2018.04.017

[6] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future Generation Computer Systems*, vol. 92, no. 1, pp. 178–188, Mar. 2019, doi: https://doi.org/10.1016/j.future.2018.09.063. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167739X18316753

[7] A. W. Ng and B. K. B. Kwok, "Emergence of Fintech and cybersecurity in a global financial centre," *Journal of Financial Regulation and Compliance*, vol. 25, no. 4, pp. 422–434, Nov. 2017, doi: https://doi.org/10.1108/jfrc-01-2017-0013

[8] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet*, vol. 11, no. 4, p. 89, Apr. 2019, doi: https://doi.org/10.3390/fi11040089

[9] N. Hassan, S. Gillani, E. Ahmed, I. Yaqoob, and M. Imran, "The Role of Edge Computing in Internet of Things," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 110–115, Nov. 2018, doi: https://doi.org/10.1109/mcom.2018.1700906. Available: https://ieeexplore.ieee.org/abstract/document/8450541.

[10] M. Demertzis, S. Merler, and G. B. Wolff, "Capital Markets Union and the Fintech Opportunity," *Journal of Financial Regulation*, vol. 4, no. 1, pp. 157–165, Jan. 2018, doi: https://doi.org/10.1093/jfr/fjx012

[11] F. Bienhaus and A. Haddud, "Procurement 4.0: Factors Influencing the Digitisation of Procurement and Supply Chains," *Business Process Management Journal*, vol. 24, no. 4, pp. 965–984, Jul. 2018, doi: https://doi.org/10.1108/bpmj-06-2017-0139

[12] J. M. Borky and T. H. Bradley, *Effective Model-based Systems Engineering*. 2019.

[13] M. Andoni *et al.*, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, no. 1, pp. 143–174, Feb. 2019, doi: https://doi.org/10.1016/j.rser.2018.10.014. Available: https://www.sciencedirect.com/science/article/pii/S1364032118307184

[14] P. Rohmeyer, J. L. Bayuk, and Springerlink (Online Service, *Financial Cybersecurity Risk Management : Leadership Perspectives and Guidance for Systems and Institutions*. Berkeley, Ca: Apress, 2019.

[15] Erdal Ozkaya, *Hands-on Cybersecurity for Finance : Identify Vulnerabilities and Secure Your Financial Services from Security Breaches*. Packt Uuuu-Uuuu, 2019.

[16] K.-K. R. Choo, "The cyber threat landscape: Challenges and future research directions," *Computers & Security*, vol. 30, no. 8, pp. 719–731, Nov. 2011, doi: https://doi.org/10.1016/j.cose.2011.08.004

[17] S. A. Bagloee, M. Tavana, M. Asadi, and T. Oliver, "Autonomous vehicles: challenges, opportunities, and future implications for transportation policies," *Journal of Modern Transportation*, vol. 24, no. 4, pp. 284–303, Aug. 2016, doi: https://doi.org/10.1007/s40534-016-0117-3. Available: https://link.springer.com/article/10.1007/s40534-016-0117-3

[18] P.-L. Pomerleau and D. L. Lowery, *Countering cyber threats to financial institutions : a private and public partnership approach to critical infrastructure protection*. Cham, Switzerland: Palgrave Macmillan, 2020.

[19] R. Baldoni and G. Chockler, *Collaborative Financial Infrastructure Protection*. Springer Science & Business Media, 2012.