Ilkogretim Online - Elementary Education Online, 2020; Vol 19 (Issue 4): pp. 7724-7740
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2020.04.765171

Cyber Security Issues Affecting Online Banking Transaction: A Thematic Analysis

Dr. Kamal Mohan Bansal Associate Professor, Department of Commerce B. R. Ambedkar College, (University of Delhi)

Abstract

The cyber security concerns influencing online banking transactions are the subject of this investigation. Cybercrimes are increasing as a result of the technology's rapid growth and widespread application in numerous industries. Online banking sectors, which include several firms, are dealing with cyber security and data breach challenges. The study of numerous technologies and methodologies used in the creation of complicated software is aided by modern computer technology. In one step, modern computing techniques can tackle problems that were challenging for traditional computing methods. They offer a new method for performing calculations. Modern computing techniques are used to create specific types of computer security techniques. Modern computing systems employ a variety of cryptographic strategies to address cyber-related problems. The largest banking system, accepted by billions of users worldwide, is mobile banking. Due to their lack of understanding, some consumers are unsure whether to accept. These days, mobile banking is thriving in the majority of developing nations thanks to its low maintenance costs and convenient internet connectivity. Most consumers attempt to communicate with their money from any location in the world. The greatest way to satiate this demand is through M-Banking. Customers can use the internet to access their bank accounts. It was also discovered that many customers occasionally need to sign in to their accounts from different devices. With so many devices logging in, hackers may be enticed to use the login history to log in. These days, mobile banking also has some positive societal consequences in the areas of governance, healthcare, agriculture, and education.

Keywords: modern computing techniques, cybersecurity issues cybercrime, cryptography, and complex software, online banking transactions.

1. Introduction

We will talk about the cyber security concerns influencing online banking transactions in this study. It may be necessary to make efforts in a variety of social, economic, and environmental areas in order to achieve competitive long-term growth and sustainability. With the aid of cutting-edge technology, even the banking industry, one of the world's most

important economic sectors, can easily achieve the global goal. As technology develops, new cybersecurity problems arise. Traditional computing methods struggle to address complex security problems. Modern computing methods are effective tools for addressing cybersecurity-related problems. Modern computing techniques have taken the place of traditional ones. The introduction of contemporary computing techniques has a significant impact on cybersecurity. A collection of strategies and techniques known as modern computing are used to address various cyber-related problems. The goal of contemporary computing technology is to make systems more resilient to cyber-related problems.

1.1 Background of the study

This study is intended to assess how internet banking works and how that has affected cyber security in general. The study defines the areas by taking into account the services for the execution of security through mobile banking. To raise awareness of cyber security risks, the idea of a knowledge gap is applied. The various chances are used to emphasise the importance of mobile banking. The study draws on ongoing research, individual motivation, skill set, and job preference. Data transmission raises concerns about the process's technology at an appropriate level. The concept of mobile banking negatively impacts the threat of cybersecurity issues. Illustrations of arithmetic knowledge get the process to explain the function of the process. The background of the research is given the functions that lead to the development of the system.

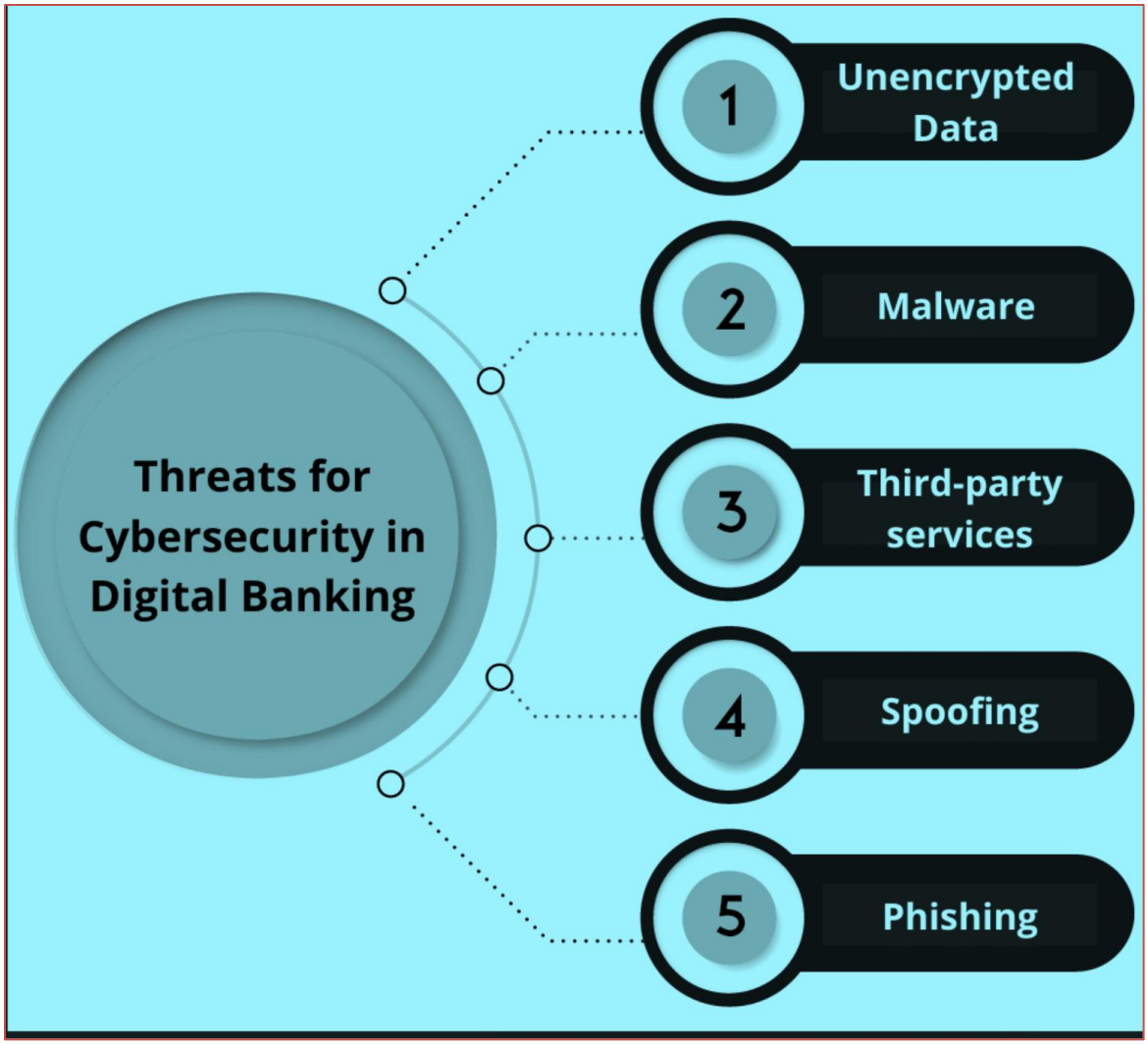

Figure 1: Challenges of cyber security related to digital banking.
(Source: Ashish M. Shaji , Jun 17, 2020)

Proving differentiated security is part of the strategy for mobile banking services. A mobile banking rating is considered a security value that helps provide information to protect your system. Various operations are used to evaluate the scope of the process. Research develops various functions such as research motivation and relevance. The growth of mobile banking strategies consists of the right opportunities for various banking institutions. Various cybersecurity issues, such as cloud attacks, ransomware attacks, phishing attacks, and various attack vulnerabilities, are affecting the capabilities of mobile banking. Process innovation and technology presuppose features related to the process framework. Process integration employs extensive knowledge and understanding of the appropriate techniques and tools for planning, investigating, and managing mobile banking systems (Wechuli et al. 2017).

Research describes future value to justify the functioning of computer knowledge. Mobile banking security risks represent processes that affect system usage. The expansion of the system is related to the various possibilities offered by information security strategies. Security assets must run in your application from your mobile device as part of the process. Exponential growth creates opportunities for further development of mobile banking services. Limited access to resources consists of the appropriate infrastructure for assessing the capabilities of cybersecurity issues. This is a powerful tool that offers a wide variety of services. According to Nambiro et al. (2017) there is a refinement of mind maps to improve their position in the computer's body of knowledge. The mind map concept is a way to link the features of mobile banking services.

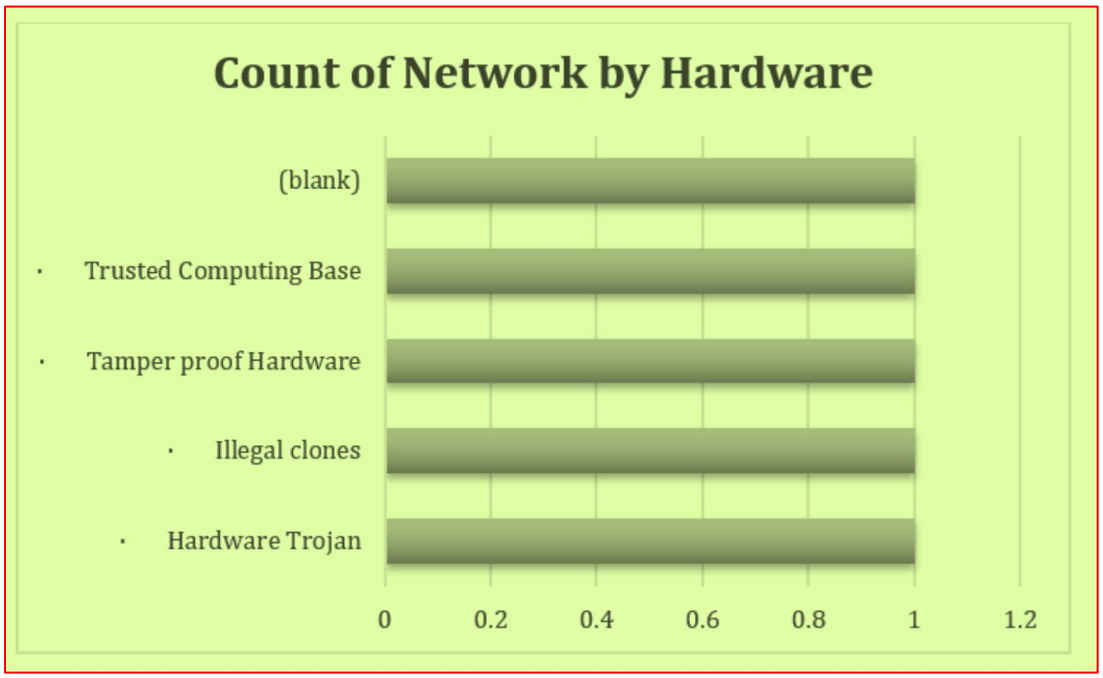

Figure 2: Adoption of Digital Banking
(Source: Nambiro et al. 2017)

The framework of online banking services estimates the function of the origin of suitable levels of approaches. The characteristics of a mind map regulate a function that is graphically expressed in the structure. The hierarchy and the association of the process are radiated to stimulate the capacity and the orientation of the process. The diagram of the mind map is shown below to facilitate the function of mobile banking services. Cyber security prevention, vulnerability, protection of information, cyber security workforce, and mobile banking service illustrate the mind map of the process.

The issues of cyber security are used to optimize the functions of mobile banking services (Zhang et al. 2018).

- ✓ Vulnerability
- ✓ Cyber Security Prevention
- ✓ Protection of Personal Information
- ✓ Cyber Security Workforce

1.2 The motivation for the study

The study is a research proposal for identifying the impact of online banking on cybersecurity issues. Online banking has become the most popular mobile commerce application used by people. As the use of mobile banking is increasing at the same time threats of cyber issues are also increasing. Various research has been conducted to find the Impact of mobile banking on cybersecurity issues. However, those researches do not completely provide the solutions to reduce the threat of cybercrimes during mobile banking. Some researchers help in identifying the issues of cybercrimes however they are failed to analyze those issues. The motivation for this study is the increasing demand for mobile banking among the public. The study will mention all the drawbacks of the previous research and provide effective solutions to reduce the risk of cyber-attacks during mobile banking. The motivation of the study is to protect the people and their financial data from cyber hackers (Coders 2017).

1.3 Relevance of the study

The study is relevant as the advancement of online banking technology has changed people's lifestyles by becoming a part of their lives. Mobile phones are not just a medium of communication however, they became an information distribution platform and are used as computing devices. The traditional banking system is being replaced by mobile e-banking which is mostly preferred by a lot of the population. In online banking, clients can easily transfer money by sharing their bank details and making an electronic bill payment anywhere. People are rapidly shifting to m-banking due to several benefits such as less time consumption, less paperwork as well as using mobile devices is convenient for them. According to Pankomera and Van Greunen (2017), the rapidly shifting the customers from traditional banking to m-banking is the relevance of this study.

Many researchers have done a study to find the impact of mobile banking on cybercrimes however they have failed to explain solutions to secure transmission of financial data to the customer's device and adapting the information to the properties of the devices (Zhang et al.2018). The study is relevant to solving these two major issues and providing secure transmission of data to customers via mobile devices. The study is relevant as the rapid shifting of the customers toward m-banking increases the rate of cybercrimes. Most of

the customers who are shifting to them-banking are not aware of the proper policies and terms and conditions of m-banking.

In this study security approach for banking is proposed to find the solutions to all three challenges. The study will provide authentication to the customer's request, and the device that is being used, and provide a secure communication channel. The study is relevant to solving the issues and challenges that are faced by the customers during banking. The study is important for the customers aware of the terms and conditions of m-banking (Ataya and Ali 2019). In this sense extensively, mobile banking has proved to be a convenient banking service through the internet. The customers in large numbers are using the facility directly via the bank's official website or by third-party payment apps (like – phone pay, Google pay, etc.) that connect the bank with the customer via mobile giving proper security. The prime cause for the huge growth of digital banking because of decreasing price of the internet along with low-cost internet-enabled Smartphones. Another reason is the easy availability of high-speed internet and good quality banking applications.

2. Literature review

2.1 Types of cybersecurity risks

The advancement in technology leads to an increase in cybercrimes. Various types of cybersecurity risks are faced by organizations, businesses, and individuals (Harel et al. 2017). It has been a prime market for malware due to the increment in the use of technology and its reliance on connectivity. Most of the common types of cybersecurity risks are malware, Traffic Interception, Phishing attacks, DDoS, Zero-day Exploit, SQL Injection, Ransomware, Crytojakcing, and MitM attacks.

Malware: It is the most common type of security threat faced by the organization. Malware is the kind of security threat when a malicious piece of software or programmer is installed in the target system that leads to unusual behavior (Khari et al. 2017). It may lead to the stealing of the information, deletion of the file, or unwanted modification in the file. It spread itself to the other files for stealing the data.

Figure 3: Types of Malwares
(Source: Khari et al. 2017)

Traffic Interception: It is also known as eavesdropping. It is the kind of security threat when the third party listens to the information shared between the sender and receiver. The data and the information shared between the host and the user get acknowledged by the third party. The data and information get stolen by the third party and stolen valuable data.

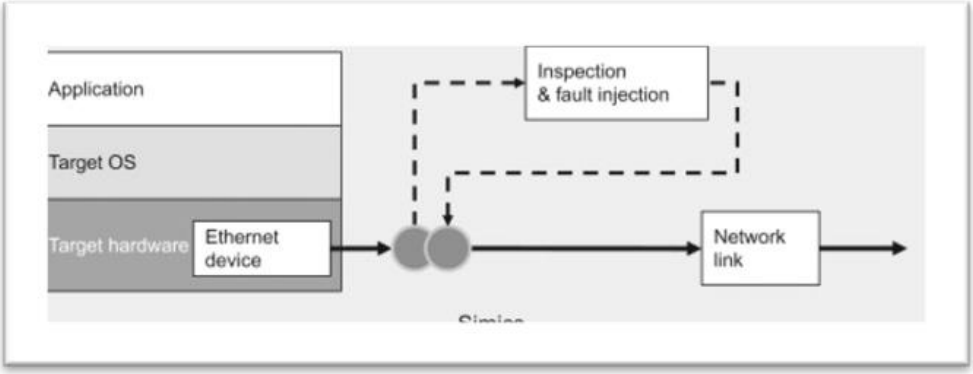

Figure 4: Traffic interception attack
(Source: created by the author)

Phishing Attacks: As per Le et al. (2019), a phishing attack is another type of cyber-attacks and this is the most common type of attack performed by hackers to steal valuable data. In this attack, the attacker sends an email to the user and requests to provide a password or any sensitive details that can lead to stealing all the sensitive information. These kinds of attacks are mostly done to steal the financial data of the individual or organization.

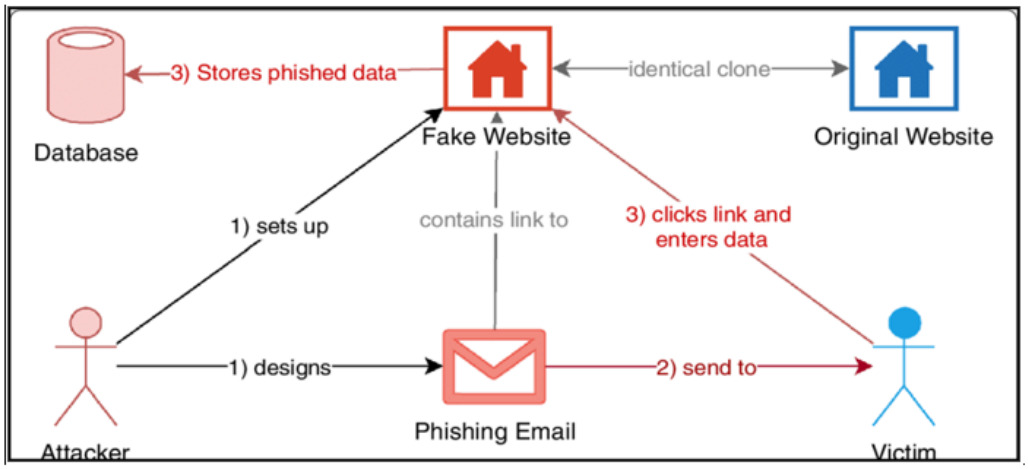

Figure 5: Phishing attack via email
(Source: Le et al. 2019)

DDoS: DDoS is known as distributed Denial of Services and it is a kind of attack which is done on the networks by overloading the traffic. The performance of users slows down due to the overloaded traffic.

Zero-Day Exploits: These kinds of cyber-attacks are done after the discovery of the "zero-day vulnerability". This kind of attack is done against the network system or software. This attack is due to the overlooked security problem in the system. These attacks damage the data as well as slow down the system and steal the information.

SQL Injection: The SQL attack is the kind of attack that manipulates the data. The third party involved in this kind of attack can manipulate the SQL queries for retrieving the sensitive information present in the system.

Ransomware: Ransomware is the kind of cyber-attack in which the ransomware installs itself in the network or the user system.

MitM Attack: It is known as A man in the Middle Attack and this kind of attack occurs when the session between the clients and host gets hijacked by a third party. With the spoofed IP address the attackers get clocks and disconnect the request and information from the clients. This type of cyber-attacks is mainly performed in banks to hack sensitive financial data (Scholefield and Shepherd 2019).

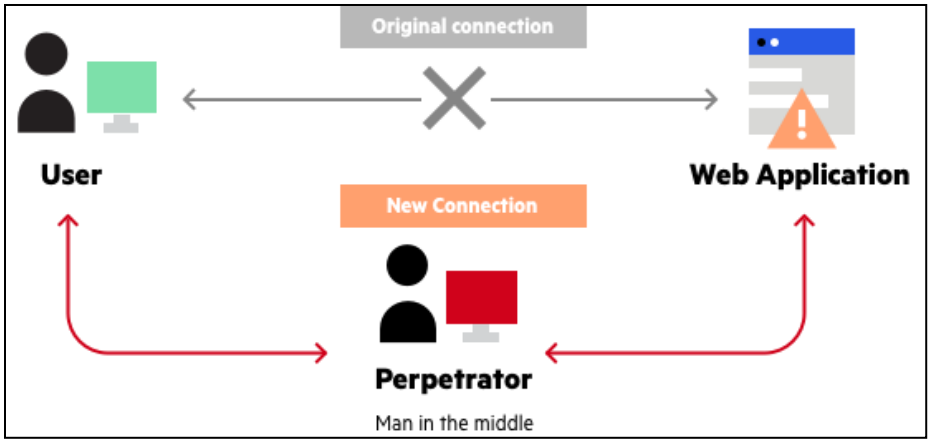

Figure 6: Man in the middle attack
(Source: Scholefield and Shepherd 2019)

2.2 Types of Modern computing platform

Various innovative technology services are built through the modern computing platform. APIs and the user interfaces for customizing, configuration, developing software, and designing are included in modern computing techniques. Various types of modern computing platforms are present for designing hardware and software. These can be high level, low level, legacy, or modern. The most common type of modern computing platform consists of a hardware platform, operating systems, client/server, mobile platform, cloud platform, Third platform, and platform as a Service (Hacioglu and Sevgillioglu 2019.

Cloud computing platform

A Cloud computing platform is a modern computing platform that is used for solving cybersecurity-related issues. Cloud platforms provide more security as it consists of various sts of policies, procedures, controls, and technologies that are used for protecting the data and infrastructure from any kind of cyber-attacks. All the cloud data get protected through the techniques provided by modern computing (Liu and Lang 2019). Cloud security is the technique used by the cloud platform to protect the stored cloud data and infrastructure. Cloud security measures are configured for protecting the cloud data and protect the customer's privacy and support regulatory compliance by setting various authentication rules for the users and devices. Cloud security is configured to filter the traffic and provide authentic access for business needs.

Cloud security is the most important technique of modern computing as it reduces the cybersecurity risk as well as manages sophisticated security threats and cloud computing can provide the best class security according to the infrastructure. The protection provided by cloud security gets centralized. Various numbers of devices are found in the cloud-based business which is difficult to manage in the case of BYOD or shadow IT.

Web filtering and traffic analysis can be enhanced through the management of these entities. software and police updates are found due to the streamlining of the monitoring and the network events. It is easy to implement disaster recovery pal when they can be managed in one place. The other benefit of using cloud security and storage is it reduces the cost involved in large hardware. The administrative overheads and capital expenditure both get reduced through the use of cloud security. As per Aldawood and Skinner (2019), cloud security provides proactive security protection to the data without the involvement of human intervention. The other benefit of cloud security is that it reduces administration. Security administration happens at one palace in the cloud security that is easily manageable and the requirement of administration gets reduced. The other main benefit of cloud security is reliability.

	Hardware	Software	Network
Common Attacks	• Hardware Trojan • Illegal clones	• Software Programming Bugs • Software Design Bugs	• Networking Protocol • Network monitoring
Examples of protections	• Tamper-proof Hardware • Trusted Computing Base	• Secure Coding Practice • Formal methods	• Firewall • Virtual Private network (VPN) • Encryption

Table 1. Examples of cyber-attacks in various ways
(Source: Thaker et al.2019, p. 758)

Data and applications can be easily accessed by users by using the right cloud security. The technology cost is getting reduced by using the cloud computing platform and more and more organizations are using this platform to solve cybersecurity issues. Force point Cloud Access Security Broker (CASB) is the cloud security solution that is used for preventing compromised accounts and it allows setting security policies based on the devices (Gupta and Sheng 2019).

2.3 Artificial Intelligence

Artificial techniques are the modern computing techniques used for cybersecurity risk. Vulnerable networks and data can be defended by using artificial intelligence by cybersecurity professionals. It has been accepted by cybersecurity experts that AI is the future of organizations. Cyber vulnerability can be easily identified by the AI as it can easily deduce the pattern and analyze the user behavior. All the kinds of irregularities and abnormalities can be easily identified by AI. At present, organizations are paying more attention to network security. As per Yavanoglu and Aydos (2017), organizations are using multiple lines of defense for securing the infrastructure and getting started with a suitable kind of filtering out of the network traffic. With the involvement of the AI, the security incidents can be easily monitored by the organization as well as with the advanced tools that can be taken.

The next-generation firewalls can easily detect the pattern in the network packets and automatically block the cyber threat to the network. AI has natural language capabilities that are used to understand the origin of a cyber-attack. This allows us to scan the data through the internet. Polymorphism and obfuscation are complicated hacking techniques that can be managed by using Machine learning AI. Machine learning is the substitute for the AI that is used as a modern computing technique for analyzing cyber threats. It can better respond to security incidents. All the malicious activities can e easily identified but the machine leading. It can easily analyze the mobile endpoints for cyber-attacks. It allows no zero-day vulnerabilities.

Deep learning AI on the cloud Video Intelligence platform is used by Google to analyze the security alerts on the contents and context of the video performed on the server of this platform. AI-powered risk prediction is used by the Babix platform that protects the IT infrastructure against security threats and data branches. In the upcoming time, AI will become the overall

2.4 Fundamentals of Genetic Programming (GP)

The major type of network attack faced is Denial of Service (DOS). The DOS attack consumed the resources of the targeted networks for not providing any services to legitimate clients. Software Toolkit is used for composing the DDOS attacks. The software allows various networks of the compromised server. It can be argued that the DDOS attacks are as same as the member of the species population, with the tactical variation similar to the biological variation. As the ineffective attacks are rarely employed and adaptation of the effective attacks helps in evading the protective mechanisms, this allows the population to arguably undergo evolutionary adaptation (i.e. variations are preset and the reproductive selection). The defensive measures have been adapted with each generation of the attack, then they have to face the next cycle of adaptation depending on the toolkit.

The defensive measures adapt or evolve with each new generation of attacks, and then they face the next cycle of adoption depending on the toolkit. A method of studying and performing attack vs defence engagements is required by cybersecurity. GP is a paradigm

for selecting and modifying the performance of units that behave. Without syntactic destruction or explicit programmer understanding, it may explore through directly modifying executable functions. Cybersecurity needs an expressively strong approach for describing the abstract assaults and responses ina way that allows for against one other in the real world. As GP can support the abstraction that can be defined such as the set of functions and terminals or as a computational language represented through the language.

3. Aims and objectives

The research aims to identify the cyber security issues found in modern computing specially in online banking.

- To identify the impact of modern computing on online banking
- To analyze the impact of modern computing on online banking affected by cyber security issues
- To find out cyber security issues found in online banking due to the use of modern computing
- To recommend solutions for overcoming the issues of cyber security

4. Materials and Methods

4.1 Methods used

Various methods were introduced in the field of modern computing techniques to address the cybersecurity issues in the organization. Some of the methods have been taken from the existing methods. The application process is known as the method used for addressing cybersecurity. The storage capacity of the get improved among network resources. DNN becomes more suitable. Spiking neural networks is the DNN technology that provides high application chances and emulates living neurons. Neural networks can be quickly developed by FPGAs which are known as Field programmable gate arrays. As per Petrenko et al. (2017), this cybersecurity is known as a cyber-attack prediction. In the field of analyzing the role of modern computing techniques, DL algorithms are mostly used. This algorithm mostly consists of generative adversarial networks, convolution neural networks, deep belief networks, stacked autoencoder, restricted Boltzmann Machines, and an ensemble of DL networks.

Modern computing techniques use expert systems that are used for the development of the software for enabling decision support to cybersecurity issues within the specific domain. Knowledge related to the domain consists of the knowledge base of the security expert system. Cyberspace, finance, or medical diagnosis are included in the application areas of the expert system. The materials used in Intelligent Agents have separate internal decision-making mechanisms and it is a self-controlled entity having a personal objective. Sensors and monitors are used for observing the threats by the actuators and controls.

Information is used by the intelligent agent to achieve objectives. Intelligent agents can easily communicate with autonomous agents.

Threat	Domestic/Foreign	Threat results
E-mail filled with virus	Origin is Foreign, domestic use	Can harm the system's Email reading capacity
Virus in network	Foreign	Have the ability to enter via unprotected ports
Web based virus	Internal views of external sites	Can affect the system and then also other internal systems
Attack on the server	foreign	If the server is hacked, then the hacker can access the internal network system.

Table 2: Threats on the servers and their consequences
(Source: Hong 2019, p. 134)

As per Mstafavi and Shafik (2019), DDoS is reduced b using the Intelligent Agent. The construction of Artificial Digital police can use the agent to prevent the DDoS attack. It rehires the implementation of the infrastructure to support the mobility of cyber agents. Another method used in modern computing techniques is Bio-Inspired Computation Methods. It is the subfield of AI and is used for the cyber that. Smart algorithms and techniques are considered for addressing the kind of cybercrime. Artificial Immune systems, Evolution Strategies, and Genetic Algorithms are the techniques that have been employed in the field of cybersecurity.

5. Result and Discussion

The result has been founded that more than 85% rate was founded for using DNN as a modern computing technique for solving the cybersecurity-related issues in the organization. Using of A.I and cloud computing have opened a new way of investigation for the organization to reduce the cyber-related challenges. As per Gupta et al. (2018), the tools provided by AI are the most effective tools against cyber threats. The complexity and number can be effectively used to protect the data against cyber-related issues.

Cybersecurity Threats(S)	Classic computing techniques	Modern computing techniques
DDoS	Uses Antivirus for detecting the flag attacks	Algorithm auto-detects abnormal network resource allocation.
Malware	Analyze monitor network traffic to spot ongoing DDoS attacks	Pattern recognition and predictive analysis to thwart new attacks
Social Engineering	Digital hygiene education and countering the hacker's tactics	Social biometrics education and ser anomaly decision
IoT and Endpoints	Cloud is used for providing manual device-level security	Analytics of network-based behavior and entity anomaly detection

Table 3: Cybersecurity threats classic computing techniques and modern computing techniques
(Source: Gupta et al. (2018, p.425)

It has been cleared from the literature review that AI and cloud security platforms can be used as a cyber domain where the classic computing methods are less effective as compared to AI. every year, the area of AI applications is published. In the given figure below the research output in the domain has been shown. It studies the time frame of AI in the field of cybersecurity. In the upcoming future, the growth of AI is going to be increased as more and more industries are switching to AI for protecting their data and infrastructure.

6. Conclusion

This study examines how contemporary computer methods relate to cybersecurity concerns in the online banking industry. Neural networks and AI are two examples of contemporary computing approaches that offer a variety of efficient tools to manage cybersecurity challenges in the enterprise. The networks and the system are damaged by numerous cybersecurity challenges, such as phishing assaults, DDoS attacks, ransomware attacks, and many others. Modern computer methods are quicker and easier to detect cybercrimes and

secure data against cybercrime than traditional computing methods. Cloud security is useful for protecting sensitive data. At the moment, artificial intelligence and machine learning enable the firm to safeguard the data against any virus assault. The study has revealed how artificial intelligence counters the cyber threat using DL and DNN. It is believed that AI would dominate all types of sectors in the near future.

7 References

Aldaej, A., 2019. Enhancing cybersecurity in modern internet of things (IoT) using intrusion prevention algorithm for IoT (Spain). IEEE Access.

Aldawood, H. and Skinner, G., 2019. Reviewing cybersecurity social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), p.73.

Ataya, M.A.M. and Ali, M.A., 2019, August. Acceptance of Website Security on E-banking. A-Review. In 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC) (pp. 201-206). IEEE.

Babu, B., Ijyas, T., Muneer, P. and Varghese, J., 2017, March. Security issues in SCADA-based industrial control systems. In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC) (pp. 47-51). IEEE.

Coders, S., 2017. The Impact of Mobile Banking On Commercial Banks in Kenya (Doctoral dissertation, United States International University-AfriAbayomi, O.J., Olabode, A.C., Reyad,

Gcaza, N., von Solms, R., Grobler, M.M. and van Vuuren, J.J., 2017. A general morphological analysis: delineating a cyber-security culture. Information & Computer Security.

Gupta, B.B. and Sheng, Q.Z. eds., 2019. Machine learning for computer and cybersecurity: principle, algorithms, and practices. CRC Press.

Gupta, B.B., Yamaguchi, S. and Agrawal, D.P., 2018. Advances in security and privacy of multimedia big data in mobile and cloud computing. Multimedia Tools and Applications, 77(7), pp.9203-9208.

Hacioglu, U. and Sevgilioglu, G., 2019. The evolving role of automated systems and its cyber-security issue for global business operations in Industry 4.0. International Journal of Business Ecosystem & Strategy (2687-2293), 1(1), pp.01-11.

Harel, Y., Gal, I.B. and Elovici, Y., 2017. Cybersecurity and the role of intelligent systems in addressing its challenges.

Khari, M., Shrivastava, G., Gupta, S., and Gupta, R., 2017. Role of Cyber Security in Today's Scenario. In Detecting and Mitigating Robotic Cyber Security Risks (pp. 177-191). IGI Global.

Khari, M., Shrivastava, G., Gupta, S. and Gupta, R., 2017. Role of Cyber Security in Today's Scenario. In Detecting and Mitigating Robotic Cyber Security Risks (pp. 177-191). IGI Global.

Le, D., Kumar, R., Mishra, B.K., Khari, M. and Chatterjee, J.M., 2019. Cyber Security in Parallel and Distributed Computing. Wiley, Hoboken.

Liu, H. and Lang, B., 2019. Machine learning and deep learning methods for intrusion detection systems: A survey. applied sciences, 9(20), p.4396.

Mendhurwar, S. and Mishra, R., 2019. Integration of social and IoT technologies: an architectural framework for digital transformation and cybersecurity challenges. Enterprise Information Systems, pp.1-20.

Mostafavi, S. and Shafik, W., 2019. Fog computing architectures, privacy, and security solutions. Journal of Communications Technology, Electronics, and Computer Science, 24, pp.1-14.

Nadikattu, R.R., 2020. New Ways of Implementing Cyber Security to Help in Protecting America. Journal of Xidian University, 14(5), pp.6004-6015.

Nambiro Alice, W., Wabwoba, F. and Wasike, J., 2017. Cyber Security Challenges to Mobile Banking in SACCOs in Kenya.

Pankomera, R. and Van Greunen, D., 2018. Challenges, benefits, and adoption dynamics of mobile banking at the base of the pyramid (BOP) in Africa: a systematic review. The African Journal of Information and Communication, 21, pp.21-49.

Petrenko, S.A., Petrenko, A.S. and Makoveichuk, K.A., 2017. The problem of developing an early-warning cybersecurity system for critically important governmental information assets. network, 4, pp.7-8.

Petrenko, S.A., Petrenko, A.S. and Makoveichuk, K.A., 2017. The problem of developing an early-warning cybersecurity system for critically important governmental information assets. network, 4, pp.7-8.

Roege, P.E., Collier, Z.A., Chevardin, V., Chouinard, P., Florin, M.V., Lambert, J.H., Nielsen, K., Nogal, M. and Todorovic, B., 2017. Bridging the gap from cybersecurity to resilience. In Resilience and Risk (pp. 383-414). Springer, Dordrecht.

Saha, M., Panda, S.K. and Panigrahi, S., 2019. Distributed computing security: issues and challenges. Cybersecurity in parallel and distributed computing: concepts, techniques, applications and case studies, pp.129-138.

Scholefield, S. and Shepherd, L.A., 2019, July. Gamification techniques for raising cybersecurity awareness. In International Conference on Human-Computer Interaction (pp. 191-203). Springer, Cham.

Tsakanyan, V.T., 2017. The role of cybersecurity in world politics. Vestnik RUDN. International Relations, 17(2), pp.339-348.

Wechuli, N.A., Franklin, W. and Jotham, W., 2017. User Perceived Secure Mobile Banking Service Provision Framework. International Journal of Computer Engineering And Information Technology, 9(10), pp.225-232.

Yavanoglu, O. and Aydos, M., 2017, December. A review on cybersecurity datasets for machine learning algorithms. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 2186-2193). IEEE.

Zhang, T., Lu, C. and Kizildag, M., 2018. Banking "on-the-go": examining consumers' adoption of mobile banking services. International Journal of Quality and Service Sciences.
https://enterslice.com/learning/cybersecurity-in-digital-banking-threats-challenges-and-solution/#:~:text=Unencrypted%20data,online%20must%20be%20fully%20encrypted.