International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Securing the Future: The Impact of AI on Cybersecurity and Economic Stability in the Banking Industry

Mohammad Waish Khan[1], Wasim Ahmad Ansari[2]

[1,2]School of Engineering, K. K. Modi University, Durg, India

ABSTRACT

People are unable to handle the volume of data and the complexity of processes required to secure cyberspace without significant automation. However, software and technologies with conventional fixed implementations are challenging to construct in order to effectively protect against security risks. AI learning techniques and machine simplicity can be used to treat this issue. And when we talk about cybersecurity in banking industry then these industries are trying to adopt artificial intelligence to develop a cyber defence system that would reduce unwanted access and cyberattacks. and how cybersecurity contributes to long-term economic growth. Meanwhile, there is a significant technological disruption taking place in the financial sector. It becomes crucial to comprehend the effects of Artificial intelligence (AI) and other technologies on the cybersecurity of banks.

Keywords: Cybersecurity, Artificial Intelligence, Data Protection, Cyber Defence Systems, Cybersecurity Challenges

1. Introduction:

Its clear that malware and cyber-arms have become significantly more complex over the last two years, it is evident that only intelligent technologies can aid in the defense against sophisticated cyber devices [1]. Network Centric Warfare (NCW) makes cyber incidents especially dangerous, and changes to cyber defense are desperately needed. Artificial intelligence approaches and knowledge-based technologies are essential for developing new offensive strategies such as dynamically establishing secure perimeters, integrating crisis management, and fully automating network assault responses [2]. Artificial intelligence, or AI, is the creation of sophisticated computer systems that mimic human mentality and are capable of carrying out tasks similar to those of a typical human being. For instance, AI systems are capable of speech recognition and language processing. AI is a broad scientific framework that includes fields of computer science, philosophy, and mathematics [3], [4]. At the same time, AI-powered cyberattacks have become more com mon, suggesting that AI can be used for both enhancing and disrupting cybersecurity Artificial intelligence presents a number of challenges since critical infrastructures are inherently unpredictable (e.g., banking industry, etc.). The majority of these concerns center on matters of security, accuracy, reliability, and safety. The main element affecting this cyber-security systems' security level is how well-defended they are against different types of cyber-attacks [5]. However, new security issues, difficulties, threats, and dangers are always appearing. One such example is the deliberate abuse of artificial intelligence technology through hacks that have the potential to cause serious harm or even death [6].

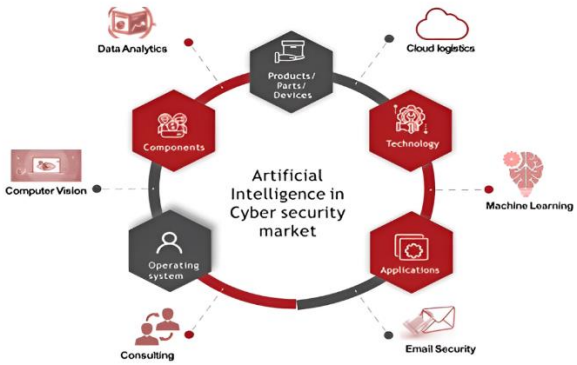

Figure 1: Usages of Artificial Intelligence [6].

one instance of a danger. Cybercriminals distributed hazardous attachments along with phishing emails. These emails were sent to the company's senior executives. a number of businesses and certain middle management personneltions. Phishing emails have been distributed, giving the impression that they are coming from the banking sector [7]. There are notes in the emails that seem to provide some advice regarding the bank payments. A SWIFT file that is attached to the email message has malicious software installed. [8]. The study makes a significant contribution to the new understanding needed to use AI security systems in business.

2. State-of-the-art

Cybercrime is the use of a computer to perpetrate crimes like theft of intellectual property and fraud. Thus, another term for digital crime is cybercrime. Attackers use a variety of methods to commit cybercrime [6]. Over a few years, there was a notable global increase in cybercrime rates that was correlated with the growth of the internet (see Table 1). Even if the platform serves as a resource for education and enjoyment, the majority of hackers use it to commit various offenses. It is now even more difficult to apprehend these criminals because of the digital method to committing a crime. When new technologies are developed, there is a rise in criminal activities on the internet [9]. This has to do with attackers coming up with fresh methods to carry out these attacks. Most governments now need to maintain a cybercrime section due to the rising incidence of cybercrime. These units make sure that the nation's level of cybersecurity has increased [9, 10]. These units have been established by several states to preserve cybersecurity in their area

Table 1: History of Cybercrimes since 2017[9]

Country	Average cybercrime cost (in millions of dollars)	Increase from 2017
United States	23.7	29%
Japan	13.5	30%
Germany	13.1	18%
United Kingdom	11.4	31%
France	9.7	23%
Singapore	9.3	n/a
Canada	9.2	n/a
Spain	8.1	n/a
Italy	8	19%
Brazil	7.2	n/a
Australia	6.8	26%

Most cybercriminals do it primarily in order to make money. The primary goal of cybercriminals is to profit by launching a specific assault against a business or a person [10].

3. Art of the State

AI has the potential to protect national secrets as well as tax cash. There are also gaps. Hackers are attempting to discover ways to get inside the devices by finding gaps in security that we were unaware of. Years go by quickly before a firm discovers a data breach [4]. An open-source system called Neural Structured Learning (NSL) trains data sets and data structures in neural nets using the Neural Graph Learning technique. NSL is intended to work for qualified machine learning specialists in addition to those who lack expertise in the field. It utilizes the Tensor Flow stage of machine learning [12].

Neural networks are the tool used by deep learning (DL) to analyze extremely complex information. AI makes it possible for the banking industry to employ cutting-edge analytical tools and creative commercial solutions. Banks can create multichannel customer access, acquire insight into consumer preferences, and customize services to meet client needs thanks to AI-powered technologies [13]. AI can identify subtle indicators that a human would have missed and halt the hacking group in their tracks. Like Varughese pointed out, anything may be misused. In the ongoing cybersecurity chess game, human hackers will always probe the weak points in any system, including artificial intelligence. Because artificial intelligence is controlled by humans, it can still be defeated. Artificial intelligence (AI) can only work as intended, despite its amazing ability to link and interpret data [14]. Since relevant legislative frameworks are still being developed, it's unclear if any company should depend on outside service providers to protect customer privacy. The use of AI-powered solutions, like chatbots for customer service or natural language processing (NLP) for staff and customer communication analysis, may violate people's privacy [15]. let's consider bank's Banks utilize a lot of AI-powered products that are connected to backend systems, where end users are clearly shown some AI capabilities. This suggests that in the context of cyber security, banks' security measures ought to take their clients' technological comfort level into consideration. This relates to the TAM (technology acceptance model), which explains user acceptance of new technologies. According to the paradigm, technology adoption is primarily driven by two factors: its usefulness and ease of use. Because of this, user behavior and the security flaws it introduces should be taken into consideration when designing cybersecurity policies for AI-powered devices [16].

AI might provide effective ways to counteract the hazards of cybercrime. Cybercrime can be prevented and detected with the help of techniques like artificial neural networks (ANNs), artificial immune systems, fuzzy logic, and genetic algorithms [17]. Businesses have employed AI to examine mobile endpoints, identify threats and thwart attacks, and supplement human analysis. [11]. There are two types of damages that banks experience after cyberattacks: direct losses and indirect losses [12]. Actual money theft and data breaches are correlated with direct losses. Poor public relations and a rise in customer annoyance and discontent present indirect losses. An examination of the magnitude of cybercrimes within developing economies' banking sectors [19].

implies that the integrity, effectiveness, and reputation of banks are negatively impacted by cybercrimes [33]. reported similar outcomes. who looked into cybersecurity in Pakistani, Indian, and Saudi online banking services. Notably, the researchers discovered that a significant proportion of banks' login pages lacked security risk information about Secure Sockets Layer (SSL), public networks, phishing, and password policies.

On the other hand, contemporary information management architecture is useful since it makes it easier for safety practitioners to assess, investigate, and comprehend cybercrime. It fortifies the digital management techniques that businesses employ to combat cybercrime and aid in maintaining the security of their clients and operations. Conversely, artificial intelligence could require a lot of resources [21]. AI is becoming a rapidly evolving area of focus for the computer safety community. We'll examine developments in AI security technologies and how the technology affects businesses, hackers, and end users. Let's resolve everything. Why it's better to have automated information security protocols online safety? Regardless of how many growing businesses you are, you have a range of security border, network, edge, device, and computer storage layers are in place [15].

In addition to network security solutions that track and identify which associated devices are authorized, you may also have firewall rules for hardware or software. The antivirus and malicious solutions will be up to the hackers if they manage to get past these security measures. They might then encounter IDS/IPS systems, etc.

Cybercrime doesn't always follow a set schedule, and it shouldn't coincide with your vulnerability to online defences. You must be able to recognize, locate, and act upon threats in real time, every day of the year. IT departments should always be prepared to respond quickly, regardless of holidays, work hours, or even when employees are just not accessible [23]. Given the quantity of AI-powered systems used in the financial sector, adversarial machine learning may pose a serious risk [18]. An ML configuration called a generative adversarial net work (GAN) is one in which an ML system is taught to identify errors in the output produced by another ML system. The progresment of GANs has enhanced AI's capacity to produce compelling "Deep fakes," or synthetic content [15]. Utilizing the decision boundaries of current ML systems is the goal of a related machine learning technique called adversarial perturbation. This makes it possible to gently alter the inputs and force the current system to give an incorrect result [17]. The presence of hostile machine learning suggests that AI-powered systems have built-in weaknesses that need to be taken into consideration while utilizing them in cybersecurity [11]. First of all, AI has the potential to be a weapon that encourages crime. For instance, hackers may use AI algorithms to find holes in security measures [17]. Second, a criminal may target an AI system directly. This is analogous to adversarial machine learning, which can be exemplified by hackers manipulating security systems to act strangely in an effort to harm. Crimes fueled by AI include video and audio impersonation, customized Phishing, interference with AI-managed systems, widespread blackmail, and data tainting [22].

4. Methods/Models Description

The ML approach and the DL method are extremely similar. As previously indicated, DL uses an automated feature selection process as opposed to a manual one, and it makes an effort to extract more detailed details from the provided data. The DBN, recurrent neural networks, and other DL programs are currently CNN and network (RNN). This section provides a description of the application of several deep neural network types to protect yourself from several network threats in various situations. One type of probability generating model is DBN, which is made up of several constrained Boltzmann layers [25]. suggested "DeepFlow," a cutting-edge DL-based method for directly detecting malware from the data flows in Android apps. This plan is executed in accordance with DBN (Fig. 2). Considering the DeepFlow design and intricate attack feature information is able to be examined. The components of DeepFlow architecture include three elements Utilizing FlowDroid to extract features SUSI for coarse-grained features and the DBN DL a categorization model. It is possible for two crawler modules to utilized to

extract malware from sources and harmless software individually from the Google Play Store [26], [27], [29].

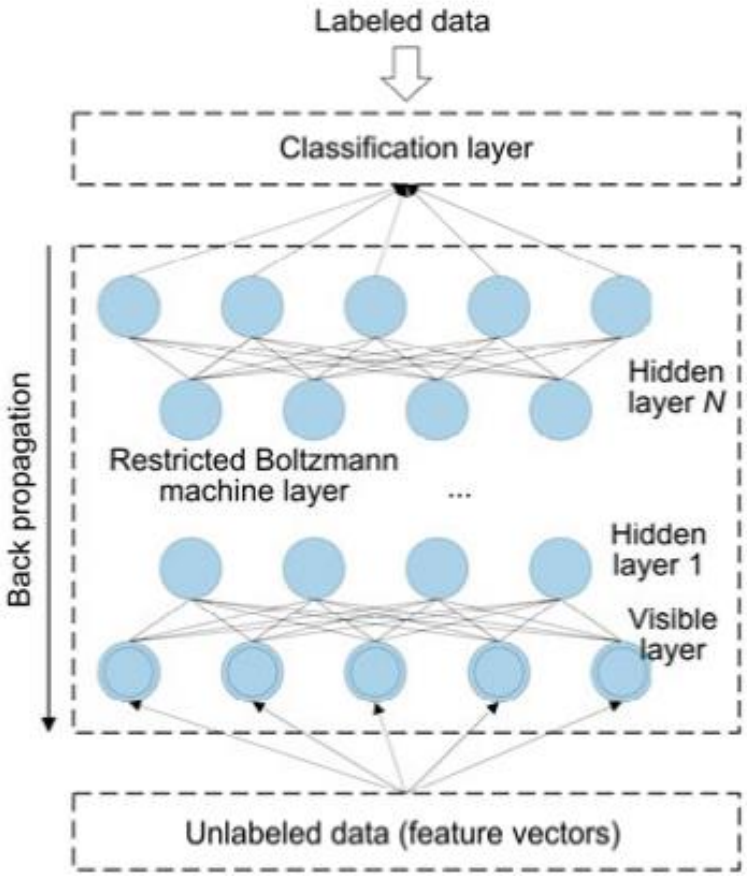

Figure 2: Deep belief network [26]

This technique transformed the raw data into low-dimensional data, from which DBN (having nonlinear learning capacity) extracted the crucial features found in the original data. They employed a Using a particle swarm optimization technique, the number of hidden-layer nodes in each layer. Subsequently, they classified the low-dimensional data using a PNN. Performance review utilizing the "KDD CUP" The "1999" dataset showed that this approach works superior to raw, PCA-PNN, and conventional PNN Without any optimization, DBN-PNN.

Safe distributed ML/DL systems

The design of privacy-preserving DL under a distributed training system, first presented by [40]. (Fig. 3), allows many parties to jointly build an accurate neural network model without disclosing the datasets used as input. This work's primary innovation is the chosen exchanging the parameters of a deep neural network while model training, which imparts effectiveness to the system and durable since asynchronous training is possible. Mobile devices can take part in the learning process in a federated learning environment, and terminal users gain from the common model that was trained on dispersed data [29]. solution was a conventional federated learning one. They offered a workable solution for DL networks in decentralized data that are communication-efficient. In light of In order to create this architecture, [30]. A workable safe aggregation strategy for high-dimensional data in machine learning that protects privacy.

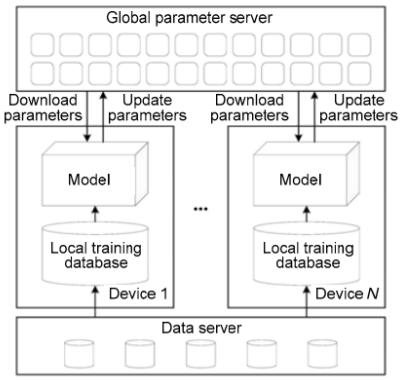

Figure 3: Safe distributed machine learning/deep learning systems [29]

Using the aggregation protocol, the server can safely calculate the total of the parameters gathered from numerous dispersed fashion across mobile devices.

5. Merits and Demerits

5.1. AI is a Major Tool for Enhancing Cybersecurity

According to the majority of respondents, banks frequently use AI-based defenses against distributed denial of service (DDoS) assaults. According to the comments, banks should use artificial neural networks and deep learning to recognize and stop web-based threats. The experts stated that because AI-based algorithms are more flexible and robust than traditional mitigation systems, they are more effective at fending off DDoS attacks. One expert said that the bank's scalable traffic analysis was done using a genetic algorithm [18]. Artificial Intelligence is bolstering cybersecurity. To start, a lot of tasks that a trained analyst would normally complete by hand may be automated with the help of AI. Identifying unknown workstations, PCs, code repositories, and other hardware parts and software on a network automatically falls under this category. The best outcomes from AI applications in cybersecurity typically occur when they are integrated with a certain level of human control [15]. In a Forbes article, Naveen Joshi, the founder and CEO of Allerin, explains how AI systems can guarantee the sustainability of cybersecurity operations in a variety of ways. Among those characteristics are:

- Creating accurate biometric password-based log-in method or methods
- Risk and suspicious activity detection using predictive analysis
- Better comprehension and reasoning through natural voice recognition
- Ensuring connection and identity through a mandate

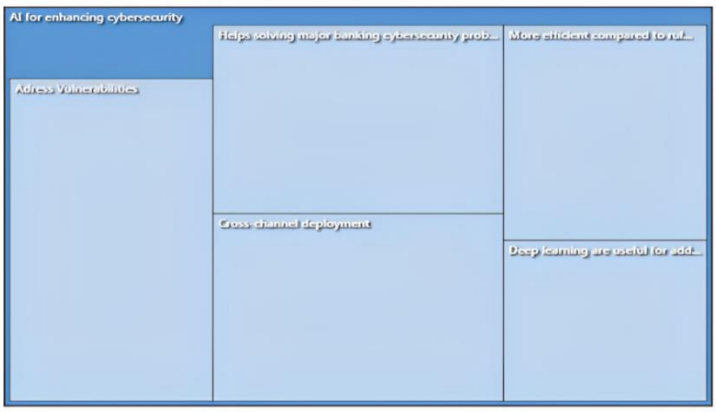

Figure 4: AI for Enhancing Cybersecurity [37]

If you ask around the industry, many of them include AI into their offerings. Major industry pioneers like are some examples of businesses who are currently using artificial intelligence cybersecurity technologies. Which are named as Palo Alto Networks, Crowd Strike, Check Point, Fortinet, Log Rhythm, Fire Eye, Sophos Symantec, etc. While artificial intelligence has numerous benefits for knowledge security, there are also hazards to consider. Applying AI to information defence tends to require more time and money than conventional, non-AI computer protection methods, which is one of the major challenges. This is partially due to the expensive nature of information protection technologies built on AI frameworks. Because of this, a number of enterprises, especially small and medium-sized ones, have historically grown to be unaffordable. However, new security-as-a-service (SaaS) technologies have emerged that increase the economic viability of AI cyber defense solutions for enterprises [20].

5.2 AI is a Tool for Threats

Physical protection is facing additional difficulties as a result of the use of AI in information defence. While it's crucial to deploy AI technology to identify and neutralize malware threats, hackers may also employ these tools to launch progressive behaviour attacks. It's also because it's becoming cheaper to produce and implement these advancements, making advanced AI technologies other than machine learning methodologies more accessible [31]. AI may potentially be used by hackers to interfere with banks' AI-powered security measures. AI might make it easier for massive w eb-based attacks, which might expose banks to extortion [24].

AI-powered crimes include data poisoning, targeted phishing, large-scale blackmail, disruption of AI-controlled systems, and audio and video impersonation. Hackers might utilize audio and video impersonation to gain access to a bank's security systems [22]. Artificial Intelligence is a phenomenon that "causes machine learning algorithms to misunderstand inputs into the framework and respond in a way beneficial to the intruder." In essence, that happens when intentionally altered inputs trick neural networks within an AI algorithm into misidentifying or incorrectly portraying things [32]. The use of cyber security may be almost limitless if the proper safeguards or precautions are not in place. Thankfully, cybersecurity experts are aware of the dangers posed by aggressive AI. According to a post on IBM's research blog for Security Intelligence, they are "building protections and making pre-emptive assault models test AI vulnerabilities." Additionally active in the project, IBM's Dublin laboratories have contributed to the ill-disposed AI index of the IBM Adversarial Robustness Toolbox (ART) [20].

6. Challenges in Using AI for Improving Cybersecurity

The creation of security measures internally was one of the frequently discussed subjects. The researchers also highlighted the difficulties the financial sector is having implementing AI, including The most frequent obstacle keeping banks from accomplishing their objectives in the use of artificial intelligence is, by far, the lack of a clear strategy [34]. First, one additional challenge that many banks encounter is a weak foundation of data and technology. The second set of issues that banks must deal with is finding employment and updating their operational plan. Artificial intelligence systems can be trained by cybercriminals, or they can introduce false information into data sets that AI uses. This will enable them to create more intricate and realistic attacks [35]. One of the biggest threats to the banking and financial sectors is ethical hacking. People are often the weakest link in data breaches because they can easily be tricked into disclosing credentials and private information. Customers and bank employees may suffer as a result of this circumstance. Artificial intelligence has a long history of unethical behavior, including invasions of user privacy, biased decisions, and AI decision-making that was unassailable. Additionally, it

is critical to identify and minimize ethical risks when developing artificial intelligence (AI) and continuing to do so after it is put into use [36]. All things considered, a key reoccurring subtheme in the expert replies is the usage of third-party software and integration. Furthermore, it appears that banks have restricted access to AI-powered communication analysis tools. When using AI technologies, a number of participants emphasized that employee and consumer privacy is crucial. It is reasonable to assume that the creation of legal frameworks like the CCPA and GDPR may be making it more difficult for banks to optimize the performance of their AI-powered systems. The comments of multiple experts who expressed concerns about privacy laws affecting the usage of AI in banks lend credence to this [26].

6.1. AI-Based Tools Have Vulnerabilities That Can Be Exploited

The weaknesses of AI-based security systems is another recurrent theme. Experts expressed special alarm about the banking industry's increasing usage of chatbots. Chatbots have the potential to leak data and pose privacy problems. According to the respondents, banks in Qatar employ conventional strategies to counter this issue, like two-factor authentication and SSL encryption. SSL guarantees the confidentiality of the data transferred across the connection. In order to use two-factor authentication, the user must retrieve a code delivered to a different device and use it to confirm their identity.

Figure 5 : Employed AI Algorithm having Vulnerabilities [37]

Although the web-based implementation of an AI-powered system is the source of the threat posed by chat bots, these systems also have intrinsic flaws. Hackers using fictitious data to install deceptive mechanics in AI engines is a serious threat. The responders listed a number of AI products, such as Teradata, Feedzai, and DataVisor, that have been employed by banks in Qatar. According to the comments, banks are tackling these innate weaknesses in AI-powered systems. According to one expert, RDBMS and the Data-Grip application are used by banks in Qatar to manage SQL databases. It is unclear, therefore, if the current management procedures take AI-based systems' data access patterns into consideration. According to a different participant, these issues would be resolved by automating processes using Security Orchestration, Automation, and Response (SOAR) software. Data buildup is a significant risk related to AI [37].

The experts' recommendations generally advise Qatari banks to handle this problem by using quantitative techniques and redundant systems. This is concerning since companies integrating Internet of Things devices and services ought to evaluate the IoT cybersecurity that their company upholds on their own [38]. As of right now, there aren't any self-assessment tools available for determining the internet of things' (IoT) cyber risk posture. The Internet of Things (IoT) is thought to be an intricate system with an excessive amount of uncontrollable risk states, making it difficult to assess risk. In complex Internet of Things (IoT)

systems, a new design has been devised and validated with comparative research to aid in the quantitative risk assessment of uncontrollable risk phases. This methodology enables the assessment of uncontrollable risk domains in intricate Internet of Things (IoT) systems that begin to mimic artificial intelligence [39].

7. Conclusion

Artificial intelligence (AI) is revolutionizing cybersecurity in the banking sector by providing powerful tools for the detection and prevention of cyberattacks. However, the successful application of AI necessitates a careful balance between innovation, ethical considerations, and strategic planning. Although AI can greatly improve security measures, it also introduces new vulnerabilities and ethical challenges. Adversarial machine learning and AI-powered cybercrimes pose significant risks that need to be addressed. In order to maximize the benefits of AI while minimizing its risks, banks must invest in research and development, put in place strong security protocols, and keep abreast of emerging threats. Ethical issues, like privacy and bias, must also be managed carefully. By taking a comprehensive approach and resolving these issues, the banking sector can use AI to create stronger, more resilient cybersecurity defences, ultimately contributing to the stability of the long-term growth of the finance sector.

References:

1. Use of Artificial Intelligence Techniques / Applications in Cyber Defense. (n.d.). Retrieved 14 August, 2020
2. Bai, J., Wu, Y., Wang, G., Yang, S. X., & Qiu, W. (2006). A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis. https://doi.org/10.1007/11760191_37.
3. AI Forum of New Zealand and AsureQuality, "Artificial Intelligence for Agriculture in New Zealand," p. 40, 2019.
4. Guerrero-Higueras, A. M., N. DeCastro-Garcıa, and V. Matellan. 2018. Detection of cyber attacks to indoor real time localization systems for autonomous robots. Robotics and Autonomous Systems 99:75–83. doi:10.1016/j.robot.2017.10.006.
5. IOS Press. (n.d.). Retrieved 14 August 2020, from https://www.iospress.nl/book/algorithms_and-architectures-of-artificial-intelligence/.
6. Bruschi, D., & Diomede, N. (2022). A framework for assessing AI ethics with applications to cybersecurity. AI and Ethics, 1-8.
7. Al-Mhiqani, M. N., R. Ahmad, Z. Z. Abidin, W. M. Yassin, A. Hassan, A. N. Mohammad, and N. L. Clarke. 2018. A new taxonomy of insider threats: An initial step in under standing authorised attack. International Journal of Information Systems and Management 1 (4):343–59. doi:10.1504/IJISAM.2018.094777.
8. Tao, Q., M. Jiang, X. Wang, and B. Deng. 2018. A cloud-based experimental platform for networked industrial control systems. International Journal of Modeling, Simulation, and Scientific Computing 09 (04):1850024. doi:10.1142/S1793962318500241.
9. Papp, D., Krausz, B., & Gyuranecz, F. (2022). The AI is now in session – The impact of digitalisation on courts. Cybersecurity and Law, 7(1), 272–296. https://doi.org/10.35467/cal/151833
10. S. Lee, (2021). AI-based Cybersecurity: Benefits and Limitations. Robotics & AI Ethics, 6(1), 18-28
11. Ghosh, A. K., Michael, C., & Schatz, M. (2000). A real-time intrusion detection system based on learning program behavior 1907, 93–109. https://doi.org/10.1007/3-540-39945-3_7.

12. IOS Press. (n.d.). Retrieved 14 August 2020, from https://www.iospress.nl/book/algorithms and-architectures-of-artificial-intelligence/.
13. Kochhar, K., H. Purohit, and R. Chutani. 2019. The rise of artificial intelligence in banking sector. In The 5th International Conference on Educational Research and Practice (ICERP) 2019(127).
14. Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., & Dehmeshki, J. (2012). An automatic approach for learning and tuning gaussian interval type-2 fuzzy membership functions applied to lung CAD classification system. IEEE Transactions on Fuzzy Systems, 20(2), 224–234. https://doi.org/10.1109/TFUZZ.2011.2172616.
15. Caldwell, M., J. T. A. Andrews, T. Tanay, and L. D. Griffin. 2020. AI-enabled future crime. Crime Science 9 (1):1–13. doi:10.1186/s40163-020-00123-8.
16. Alghazo, J. M., Z. Kazmi, and G. Latif. 2017. Cyber security analysis of internet banking in emerging countries: User and bank perspectives. In 2017 4th IEEE international confer ence on engineering technologies and applied sciences (ICETAS) (1–6). IEEE. doi:10. 1109/ICETAS.2017.8277910.
17. Dilek, S., H. C¸akır, and M. Aydın. 2015. Applications of artificial intelligence techniques to combating cyber-crimes: A review. arXiv Preprint arXiv:1502.03552
18. Geluvaraj, B., P. M. Satwik, and T. A. Ashok Kumar. 2019. The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace (739–47). Springer, Singapore.
19. Akinbowale, O. E., H. E. Klingelh€ ofer, and M. F. Zerihun. 2020. Analysis of cyber-crime effects on the banking sector using the balanced score card: 27 (3):945–58. doi:10.1108/JFC-03-2020-0037.
20. Lai, S. T., F. Y. Leu, and J. W. Lin. 2018. A banking chatbot security control procedure for protecting user data security and privacy. (561–71). Springer, Cham, October
21. Kotkas, V., Penjam, J., Kalja, A., & Tyugu, E. (2013). A model-based software technology proposal. MODELSWARD 2013 - Proceedings of the 1st International Conference on Model Driven Engineering and https://doi.org/10.5220/0004348203120315. S
22. Pachghare, V. K., Kulkarni, P., & Nikam, D. M. (2009). Intrusion detection system using self organizing maps. 2009 2009, 4(12), 11–16. https://doi.org/10.1109/IAMA.2009.5228074.
23. Parati, N., & Anand, P. (2017). Machine Learning in Cyber Defence. International Journal of Computer Sciences and Engineering, 5(12), 317–322.
24. Kaloudi, N, and J. Li. 2020. The AI-based cyber threat landscape: A survey. ACM Computing Surveys 53 (1):1–34. doi:10.1145/3372823.
25. Zhu DL, Jin H, Yang Y, et al., 2017. DeepFlow: deep learning-based malware detection by mining Android application for abnormal usage of sensitive data. IEEE Symp on Computers and Communications, p.438-443. https://doi.org/10.1109/ISCC.2017.8024568.
26. Ota K, Dao MS, Mezaris V, et al., 2017. Deep learning for mobile multimedia: a survey. ACM Trans Multim Comput Commun Appl, 13(3S), Article 34. https://doi.org/10.1145/3092831
27. Li LZ, Ota K, Dong MX, 2018a. Deep learning for smart industry: efficient manufacture inspection system with fog computing. IEEE Trans Ind Inform, 14(10):4665- 4673. https://doi.org/10.1109/TII.2018.2842821
28. Li LZ, Ota K, Dong MX, 2018b. DeepNFV: a light-weight framework for intelligent edge network functions virtualization. IEEE Netw, in press. https://doi.org/10.1109/MNET.2018.1700394.
29. McMahan HB, Moore E, Ramage D, et al., 2016. Communication-efficient learning of deep networks from decentralized data. https://arxiv.org/abs/1602.05629.

30. Bonawitz K, Ivanov V, Kreuter B, et al., 2017. Practical secure aggregation for privacy-preserving machine learning. Proc ACM SIGSAC Conf on Computer and Communications Security, p.1175-1191.
31. Rosenblatt, F. (1957). The Perceptron - A Perceiving and Recognizing Automaton. In Report 85, Cornell Aeronautical Laboratory (pp. 460–461). https://doi.org/85-460-1.
32. Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial Intelligence in Cyber Security 06(05), 01–07. https://doi.org/10.31695/ijerat.2020.3612.
33. Rammanohar Das and Raghav Sandhane 2021, Artificial Intelligence in Cyber Security, Journal of Physics: Conference series , 1964 042072
34. Ranjan, S., D. R. Gupta, and D. A. Gupta. 2020. Artificial intelligence in financial acumen: Challenges and opportunities. Cosmos Journal of Engineering & Technology 10 (1):1–5.
35. Thowfeek, M. H., S. N. Samsudeen, and M. B. F. Sanjeetha. 2020. Drivers of artificial intel ligence in banking service sectors. Solid State Technology 63 (5):6400–11.
36. Ryzhkova, M., E. Soboleva, A. Sazonova, and M. Chikov. 2020. Consumers' perception of artificial intelligence in banking sector. In SHS Web of Conferences 80:1019. EDP Sciences. doi:10.1051/shsconf/20208001019
37. Khalifa AL-Dosari, Noora Fetais & Murat Kucukvar 2024, Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges taylor & Francis 55:2, 302-330, DOI:10.1080/01969722.2022.2112539
38. Radanliev, P, and D. De Roure. 2021. Review of algorithms for artificial intelligence on low memory devices. IEEE Access. 9:109986–93. doi:10.1109/ACCESS.2021.3101579.
39. Cerrudo, C, and L. Apa. 2017. Hacking robots before skynet. IOActive Website 1–17.
40. Shokri and Shmatikov 2015, Privacy-Preserving Deep Learning, *CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*
41. *Muhammad Shoaib Akhtar1 and Zhang Jiayuan1 2021, The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey doi: 10.4108/eai.7-7-2021.170285*