THREATS AND OPPORTUNITIES WITH AI-BASED CYBER SECURITY INTRUSION DETECTION: A REVIEW

Bibhu Dash, Meraj Farheen Ansari, Pawankumar Sharma and Azad Ali

Dept. of Computer and Information Systems,
University of the Cumberlands, Williamsburg, KY USA

ABSTRACT

Internet usage has increased quickly, particularly in the previous decade. With the widespread use of the internet, cybercrime is growing at an alarming rate in our daily lives. However, with the growth of artificial intelligence (AI), businesses are concentrating more on preventing cybercrime. AI is becoming an essential component of every business, affecting individuals worldwide. Cybercrime is one of the most prominent domains where AI has begun demonstrating valuable inputs. As a result, AI is being deployed as the first line of defense in most firms' systems. Because AI can detect new assaults faster than humans, it is the best alternative for constructing better protection against cybercrime. AI technologies also offer more significant potential in the development of such technology. This paper discusses recent cyber intrusions and how the AI-enabled industry is preparing to defend itself in the long run.

KEYWORDS

AI, cybercrime, cyberattacks, machine learning, cybersecurity, security analytics, classification.

1. INTRODUCTION

Artificial Intelligence is becoming the next technological movement across most industries. The past few years have showcased different industries engaging different services through the help of AI [1]. The various applications associated with AI have enabled it to be applied in several industries today. The influence related to these applications has contributed to increased confidence in AI technologies. The idea of AI being in cybersecurity has also been applied through very effective systems [2]. Most of these systems have recorded increased benefits and effectiveness by using AI. The overall adoption of AI in building a defense against cybercrime has therefore been tested and deemed effective [2]. AI algorithm is consequently essential in building a solid defense against cybercrime.

1.1. Background in Cybercrime

Cybercrime is using a computer to commit crimes such as fraud and intellectual property theft. Cybercrime is, therefore, another name given to computer crime. There are several ways through which attackers engage in cybercrime [2]. Internet development was associated with a significant increase in cybercrime rates across the globe over a few years (see Table 1). Despite being an educational and entertainment tool, most hackers use the platform to engage in different crime levels. The digital approach to accomplishing a crime has made it even harder to catch these perpetrators. Criminal activity across the internet increases with the development of every technology [3]. This is associated with attackers finding newer ways to accomplish these attacks.

The growing rates of cybercrime have created the need for most governments to include a cybercrime unit [3] [4]. These units ensure that cybersecurity has been increased across the country [4]. Different states have developed such units to maintain cybersecurity in their regions.

Table 1. History of Cybercrimes since 2017

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%

The main reason for conducting cybercrime for most attackers is to obtain a profit. Cybercriminals always focus on making a profit by using a defined attack on a company or another individual [4]. Each of these different types of attacks always focuses on the criminal's financial gain [5] see figure.2 below. A good example is a ransomware attack which ensures that the victim has paid a defined amount of money as directed by the criminal [5]. Companies also consistently participate in cybercrime to remain further than their competitors.

The US department of justice has divided cybercrime into three main categories. The first category focuses on the device itself, the second attacks are those used as a weapon against an organization, and the third type is those attacks where a computer is an accessory to the crime [6]. Cybercriminal activity majorly focuses on the three areas described. Cyberattacks can also be achieved in several ways. Some standard methods of achieving attacks include DoS attacks, phishing attacks, identity theft, software piracy, and cyber espionage, among others [6]. Each episode has key processes the attackers must use to access the information they require. Each of these cybercrimes includes a set of steps that can be included in achieving protection against it.

Cybercrime has embraced AI technology to accomplish its critical attacks [7]. The interest in conducting successful attacks has seen more innovative ways of boosting cybercrime. Some phishing attacks have been seen to engage social engineering via AI technology. These attacks furthermore showcase the demand for AI in anti-phishing algorithms. It confirms that procedures can safeguard against attacks with an identical or more productive strategy. This also showcases the capabilities of anti-phishing algorithms [8].

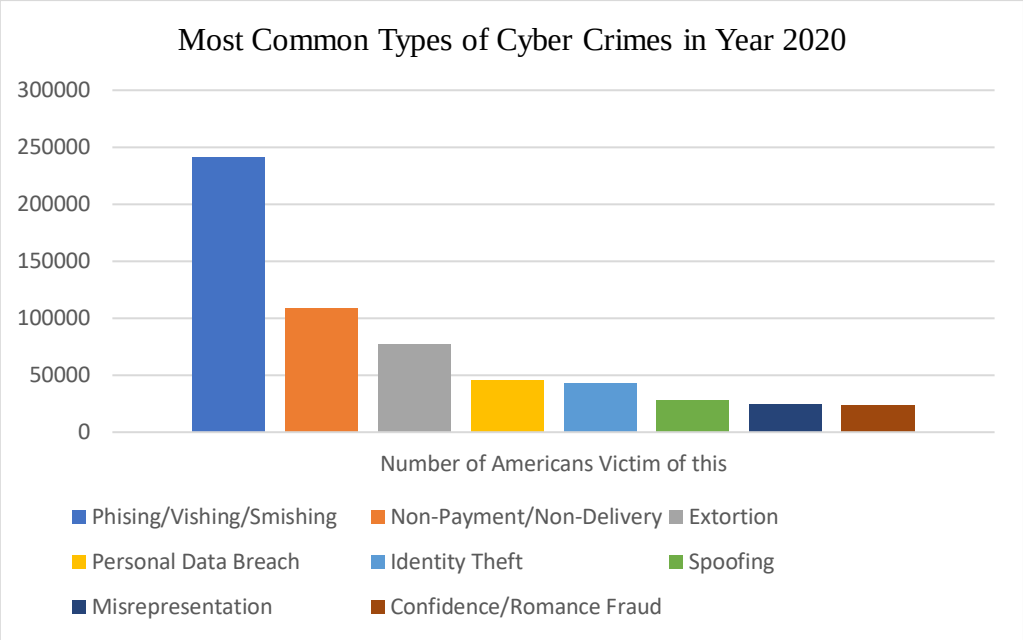

Figure 1. Types of Cybercrime in North America in the Year 2020

Cybercrime has several effects on businesses in general. The below figure.3 depicts the impact of the $600 billion loss experienced in 2018 due to global cybercrimes [6]. These numbers indicate that cybercrimes are a growing menace to the community in general. Therefore, finding an effective solution to this issue is essential [7]. Companies suffer greatly from cyber criminals, requiring the need to update their security protocols. The overall effects of cybercrime have also been found to impact national security. Finding protections against cybercrime is therefore of interest to companies and nations.

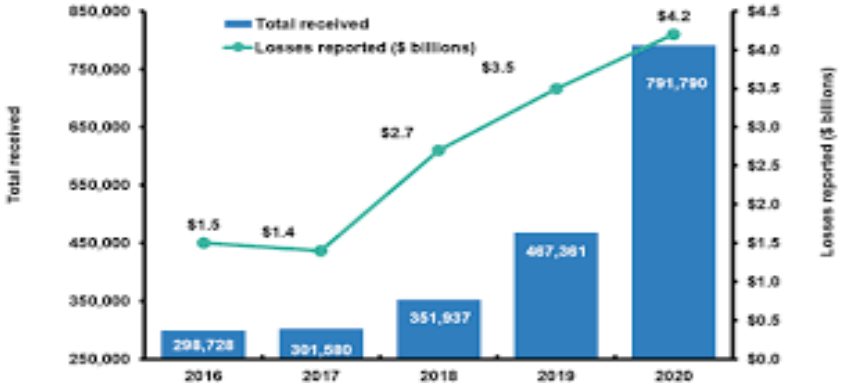

Figure 2. Cybercrime Statistics [6]

1.2. Adopting AI in Cybersecurity

Artificial intelligence has become an essential part of most industries today. The growth of cybersecurity within different industries has been associated with the list of applications related to AI. AI has increasingly been adopted in businesses by promoting automation. Automation has primarily focused on increasing productivity and limiting human influence [8] [4]. AI has, however, begun to be engaged in data analysis and security. Data security is a growing concern

cybersecurity. It ensures that the digital transformation has continued to improve [8]. Estimates have suggested that the global market for AI in cybersecurity will reach 46.3 billion dollars by 2027 [8]. This indicates a growing inclusion of AI in cybersecurity [9].

AI is considered more applicable in data security because of the possibility of automation [9]. The inclusion of automation means that AI systems can include immediate protection immediately after an individual tries to access this data. Several factors are associated with AI being an essential part of cybersecurity [10]. Most of these characteristics are related to the features of AI technology in the community today [10]. Therefore, the growing need for this technology has remained an important reason for including AI as a form of security.

The main characteristic of AI technology being included in cybersecurity is its ability to detect. AI automation makes it an effective technology in detection [11]. AI systems could be programmed to detect specific steps and behavior and sound an alarm if available [12]. Since AI systems can monitor the system 24/7, they are considered very effective detection systems [13].This factor is why most organizations have implemented AI-based security protocols [13] see figure.4. Different network firewalls also include AI algorithms as security measures against cyber criminals [14].

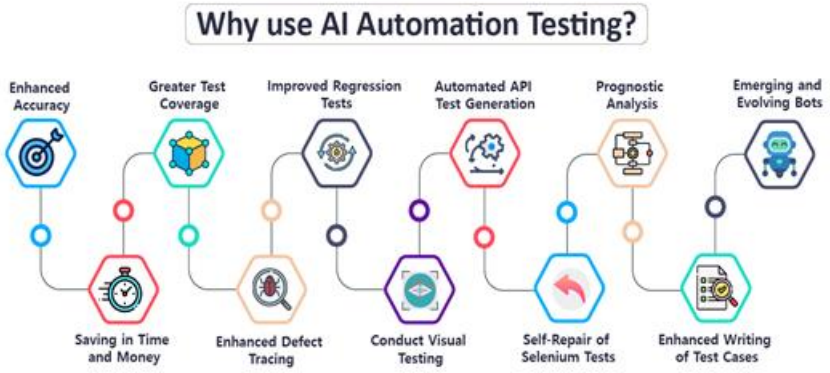

Figure 3. Automation Testing [13]

The following characteristic of AI technology in cybersecurity has been its ability to predict threats. The prediction has been considered one of the characteristics and applications of AI technologies [14]. This characteristic has been associated with the power of AI technology to analyze large amounts of data in a short while [8]. The AI system can continually be developed in a specific method to ensure that it explores the data provided and makes different predictions based on the system's training [15]. The development of machine learning has enabled this ability to be achieved [7]. Therefore, AI systems in cybersecurity engage in data analysis focused on predicting cyber threats see figure. 5. This approach also ensures cybersecurity has been achieved.

The final characteristic of AI technology's effectiveness in cybersecurity is its response time [16] see figure.6. AI algorithms are implemented in cybersecurity because of their fast response time [7]. Despite being effective, cybersecurity analysts do not always respond quickly to attacks. The ability of AI systems to learn and analyze situations faster makes them even more effective in responding to such conditions [16]. This ability ensures that the system or network has not been compromised [16]. Cybersecurity systems can therefore include AI algorithms to ensure that the response time has increased significantly and that data has remained protected.

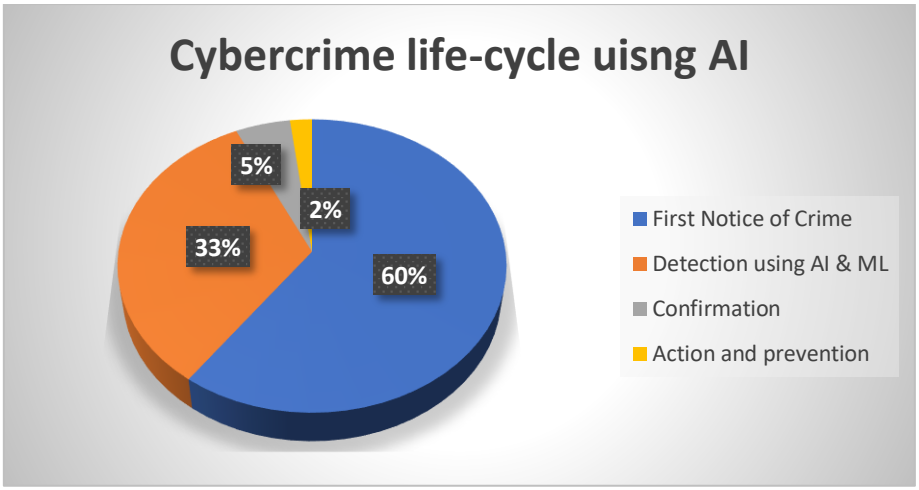

Figure 4. Cybercrime lifecycle using Predictive Analytics & ML [15]

Machine learning technology in AI has also promoted the inclusion of AI in cybersecurity. Machine learning is an integral part of AI technology [16]. The technology includes learning ability in AI systems. These technologies are essential when developing a high-end cybersecurity system [17]. Developing strategies that can learn in run time is considered a practical approach due to the speed needed in defending against attacks. Machine learning technology ensures that a defense system has studied the attacker's methods and engages newer approaches to defend against these attacks [17]. Engaging in such solutions provides that the attacker is unsuccessful in completing any attacks they have on an organization or company.

Each of the properties described above is considered essential in the ability of AI systems to defend against cybercriminals. Including each of the properties above ensures that a system has remained safe from criminals. Each cyberattack described before is increasingly ineffective when engaging in effective protection methods, as showcased before. Therefore, AI use in cybersecurity has recorded several results from AI's properties towards the technologies present [8]. This has also contributed to several advantages of AI technology in protecting different organizations [8]. The various properties described also showcase the critical reason why AI technology is being appreciated in cybersecurity. Therefore, preparing a solid defense through an AI algorithm is practical. Some organizations implementing the algorithms have indicated an increase in the quality of defense offered [13] [17]. The defense is considered more successful because of the ability of the technology to maintain high-level security [17]. The AI tools, such as machine learning, also indicate the effectiveness of preparing a strong defense against cybersecurity through AI algorithms. The properties of AI are, therefore, the main contributing factor resulting in its efficacy in achieving AI technology.

2. CHALLENGES OF AI IN CYBER SECURITY

Despite the benefits associated with AI in cybersecurity, there are several challenges and disadvantages which affect its development. The drawbacks and limitations have been the main factor limiting an increased adoption of AI in cybersecurity [18, 19].

2.1. AI and its usability by Criminals

The first challenge associated with AI is its use by cybercriminals [4]. AI can therefore be regarded as a double-edged sword [19]. The technology is considered a limiting factor because

attackers can obtain the AI systems and study them to understand their vulnerabilities [18]. This action will therefore make their attacks more precise and successful. With the rise of big data technologies and spark engines, analyzing unstructured data for cyber threats using AI models is more convenient now than before [18].

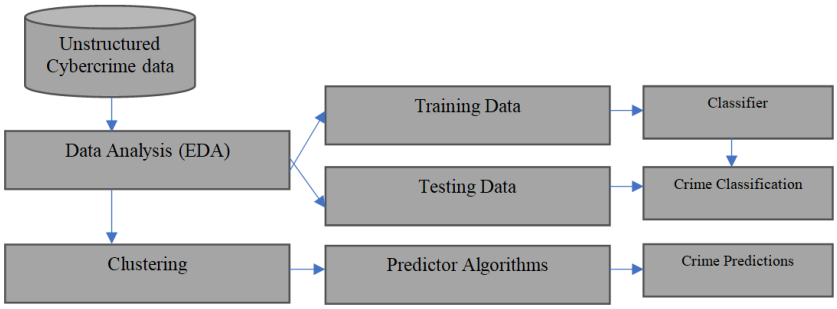

Figure 5. An AI analyzer to classify cybercrime threats

Most cyber criminals have also used AI in achieving specific attacks. Cybercriminals can obtain AI algorithms in their systems and complete their defined attacks [4]. AI has mainly been found to be very effective in finding vulnerabilities in application software [18]. The attackers could then use the exposures obtained to gain access to the company [7]. The overall approach of using AI is to provide cyber criminals with an advantage against cybersecurity [18]. This advantage has been a continued reason for the increased cybercriminal activity and why there is a decreased adoption of AI in cybersecurity.

When data scientists and cybersecurity specialists collaborate, they may create a more generalizable model. As IT professionals evaluate an AI-powered cybersecurity solution, what counts and where machine learning can flourish is catching new, unexpected threats. Let's use the equations below as an example to highlight one detail in verifying a model and its statistics for this purpose.

Precision is the ratio of correctly anticipated positive samples to the total number of correctly predicted positive samples. If the accuracy score is higher, our model is doing an excellent job of classifying the data.

$$\text{Precision} = \frac{TP}{TP+FP} \qquad (1)$$

Recall: It is the proportion of actually anticipated positive samples in the actual class that are present. It is also known as the model's sensitivity.

$$\text{Recall} = \frac{TP}{TP+FN} \qquad (2)$$

F1 Score: The F1 score is determined by taking the weighted average of accuracy and recall. True negatives, true positives, false negatives, and false positives are its key components (considerations). The F1 score is chosen above accuracy to understand the AI-based classifier model performance metric.

$$\text{F1 Score} = 2 \times (\text{precision} \times \text{recall}) \qquad (3)$$

$$\text{Accuracy} = \frac{TP+FN}{TP+FN+TN+FP} \qquad (4)$$

Researchers compute the end outcomes in terms of precision, recall, F1 score, and total accuracy, as specified above, to assess the performance of AI-based cyber security models. In the following formal definitions of precision, recall, F1 score, and total accuracy, TP signifies true positives, FP means false positives, TN denotes true negatives, and FN denotes false negatives.

2.2. AI Adaptability in an Organizational Setup

Another critical limitation of AI in cybersecurity has been the adoption factors. AI could be considered a very new technology [8]. There is a considerable lack of awareness of the potential of AI. Being a growing technology has been considered a limiting factor by most organizations in adopting the technology in their companies [18, 19]. AI also requires significant investments from these organizations [4]. The investment could also contribute to the adoption barriers by most organizations. The limited technologies, therefore, mean that their popularity in cybersecurity is also shallow [7]. This challenge needs to be resolved by increasing the awareness of the potential of this technology. This action will contribute to the adoption of AI and engage more research into the sector.

Despite the limitations and challenges described above, AI is still a considerate technology in cybersecurity defense systems [4]. The technology has reportedly prevented attacks from different attackers [2]. The technology can be programmed into a cybersecurity system and be able to fend off different types of seizures [2]. This factor has made them cheaper to hire specialists [8]. The technology is also regarded as the best potential for preparing a strong defense due to its inability to make mistakes similar to those humans could make.

3. FUTURE OF CYBER SECURITY

More schools have been seen to include AI training across their institutions. The need for AI specialists has increased over the past decade due to their rising applications. Cybersecurity specialists are also urged to engage in skills in AI [19]. Each of these factors indicates the future of AI in cybersecurity is growing [4]. Increased awareness promotes the development of AI defenses across cybersecurity [19, 20, 21]. These approaches will ensure cybersecurity defenses have become wholly automated shortly.

Therefore, the trend associated with AI inclusion in cybersecurity promises a bright future for AI-based cybersecurity. Companies are also urged to implement the technology because of its effectiveness in promoting security [19]. Engaging in a defined type of security is a crucial requirement for most users [4]. The technologies being included will therefore increase the level of development required for developing AI systems that offer cybersecurity [22]. Cyberattacks have also been seen to adopt AI algorithms [23] increasingly. This factor has resulted in the need for cybersecurity defenses to include AI [24-26]. This is related to AI technology's capabilities being the best protection against a similar AI-based attack. When employing AI for cybercrime and dealing with personal identity thefts, PII data is most safe with the establishment of a federated learning [27]. As a result, using AI-based systems to guard against cyberattacks leads to the best defense in the modern digitalization era.

4. CONCLUSION

This paper examined scenarios for an intrusion detection machine-learning-based security model. Good protection against cybercrime requires an AI algorithm. Detection, prediction, and response time skills are among the several features discussed. Companies should consequently continue to use AI algorithms to adopt cybersecurity safeguards. As a result, businesses and consumers

should recognize that establishing a robust defense against cybercrime is best accomplished with AI technology. Future research might assess the study's usefulness by collecting large datasets with more dimensions of security features in IoT security services and examining its efficacy at the application level in cybersecurity.

REFERENCES

[1] Shindo, T., Kimura, T., & Hiraguri, T. (2021). Defense against DoS attacks by multipath routing using the ACO algorithm. *IEICE Communications Express*.

[2] Bruschi, D., & Diomede, N. (2022). A framework for assessing AI ethics with applications to cybersecurity. *AI and Ethics*, 1-8.

[3] 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

[4] S. Lee, (2021). AI-based Cybersecurity: Benefits and Limitations. *Robotics & AI Ethics*, *6*(1), 18-28.

[5] Kim, J., & Park, N. (2020). Blockchain-based data-preserving ai learning environment model for ai cybersecurity systems in IoT service environments. *Applied Sciences*, *10*(14), 4718.

[6] Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2019). Blockchain and AI for the next generation energy grids: cybersecurity challenges and opportunities. *Information & Security*, *43*(1), 21-33.

[7] Furqan, M. (2021, April 25). The Most Common Types of Cyber Crime. Lifeboat Foundation Safeguarding Humanity. Retrieved July 24, 2022, from https://lifeboat.com/blog/2021/04/the-most-common-types-of-cyber-crime

[8] Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques – a review of Cyber Defense Mechanisms. IJARCCE, 11(7). https://doi.org/10.17148/ijarcce.2022.11728

[9] Dymicka, A. (2022). Cybersecurity from the perspective of a new technology user. Cybersecurity and Law, 7(1), 27–36. https://doi.org/10.35467/cal/151810

[10] Qumer, S. M., & Ikrama, S. (2022). Poppy Gustafsson: redefining cybersecurity through AI. *The Case for Women*, 1-38. https://doi.org/10.1108/cfw.2022.000001.

[11] Tagarev, T., Stoianov, N., Sharkov, G., & Yanakiev, Y. (2021). AI-driven Cybersecurity Solutions, Cyber Ranges for Education & Training, and ICT Applications for Military Purposes. *Information & Security*, *50*(1), 5-8. https://doi.org/10.11610/isij.5000.

[12] Biasin, E., & Kamenjašević, E. (2022). Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. *International Cybersecurity Law Review*, 1-18.

[13] Senouci, S. M., Sedjelmaci, H., Liu, J., Rehmani, M. H., & Bou-Harb, E. (2020). Ai-driven cybersecurity threats to future networks [from the guest editors]. *IEEE Vehicular Technology Magazine*, *15*(3), 5-6.

[14] Liu, X. M., & Murphy, D. (2020). A Multi-Faceted Approach for Trustworthy AI in Cybersecurity. *Journal of Strategic Innovation & Sustainability*, *15*(6).

[15] Stevens, T. (2020). Knowledge in the grey zone: AI and cybersecurity. *Digital War*, *1*(1), 164-170. https://doi.org/10.1057/s42984-020-00007-w.

[16] Puthal, D., & Mohanty, S. P. (2021). Cybersecurity issues in AI. IEEE Consumer Electronics Magazine, 10(4), 33-35.

[17] Hamilton, T. (2022, June 25). What is response time testing? how to measure for API, Tools. Guru99. Retrieved July 30, 2022, from https://www.guru99.com/response-time-testing.html.

[18] Dash, B. (2021). A hybrid solution for extracting information from unstructured data using optical character recognition (OCR) with natural language processing (NLP).

[19] Tsvilii, O. (2021). Cyber Security Regulation: Cyber Security Certification of Operational Technologies. *Technology audit and production reserves*, *1*(2), 57.

[20] Timmers, P. (2019). Ethics of AI and cybersecurity when sovereignty is at stake. *Minds and Machines*, *29*(4), 635-645.

[21] Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. In *Journal of Physics: Conference Series* (Vol. 1533, No. 3, p. 032014). IOP Publishing.

[22] Bowman, B., & Huang, H. H. (2021). Towards Next-Generation Cybersecurity with Graph AI. *ACM SIGOPS Operating Systems Review*, *55*(1), 61-67.

[23] Grochmalski, P. (2021). Nowy Paradygmat Bezpieczeństwa A AI. Cybersecurity and Law, 1(1), 93–113. https://doi.org/10.35467/cal/133772

[24] Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. Prevention. https://doi.org/10.47893/IJSSAN.2022.1221
[25] Grabosky, P. (2016). The evolution of cybercrime, 2006–2016. In *cybercrime through an interdisciplinary lens* (pp. 29-50). Routledge.
[26] Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.
[27] Dash, B., Sharma, P., & Ali, A.(2022). FEDERATED LEARNING FOR PRIVACY-PRESERVING: A REVIEW OF PII DATA ANALYSIS IN FINTECH. https://doi.org/10.5121/ijsea.2022.13401

AUTHORS

Bibbu Dash is a data Architect in a Fortune 100 financial organization in Madison, WI. He is currently a Ph.D. scholar in Information Technology at the University of the Cumberlands, Kentucky. Bibhu has completed his Master of Engineering in Electronics and Communication Engg. and MBA from Illinois State University, Normal, IL. Bibhu's research interests include AI, Cloud Computing, Big Data, and Blockchain technologies.

Dr. Meraj Farheen Ansari completed her Ph.D. (IT) from the Graduate School of Information Technology, University of the Cumberlands. She also completed her MBA with a Specialization in Management Information Systems from Concordia University, Milwaukee, WI, USA. Her research interests include cybersecurity awareness, eliminating Cyber Threats, & ML. Her current research involves making organizational employees aware of cyber security threats using AI awareness programs. Currently, she is a Cyber Security Analyst at Northern Trust Bank, Chicago, IL.

Pawankumar Sharma is a Senior Product Manager for Walmart in San Bruno, California. He is currently on his Ph.D. in Information Technology at the University of the Cumberlands, Kentucky. Pawankumar completed his Master of Science in Management Information Systems from the University of Nebraska at Omaha in 2015. He also holds another Master of Science in Information Systems Security from the University of the Cumber lands, Kentucky, and graduated in 2020. His research interests are cyber security, Artificial Intelligence, Cloud Computing, Neural Networks, Information Systems, Big Data Analytics, and Intrusion Detection and Prevention.

Dr. Azad Ali, D.Sc., Professor of Information Technology, has more than 30 years of combined experience in financial and information systems. He holds a bachelor's degree in Business Administration from the University of Baghdad, an MBA from the Indiana University of Pennsylvania, an MPA from the University of Pittsburgh, and a Doctor of Science in Communications and Information Systems from Robert Morris University. Dr. Ali's research interests include service-learning projects, web design tools, dealing with isolation in doctoral programs, and curriculum development. Azad has been involved in mentoring postgraduate students to complete their doctoral dissertations and has so far mentored five students to complete their dissertations.