rice2024 Proceedings of the Ninth International Conference on Research in Intelligent Computing in Engineering pp. 71–77
DOI: 10.15439/2024R34
ISSN 2300-5963 ACSIS, Vol. 42

Harnessing AI for Enhanced Identity Management: Addressing Cybersecurity Challenges in the Digital Age

Suman Thapaliya
Department of Information Technology
Lincoln University College
mailsumanthapaliya@gmail.com

Sudan Jha
Department of Computer Science and Engineering
Kathmandu University
jhasudan@ieee.org

***Abstract*—The integration of Artificial Intelligence (AI) into cybersecurity has significantly advanced identity management, particularly in combating Account Takeover (ATO) and enhancing digital security. Traditional cybersecurity methods often fail to keep up with the dynamic nature of cyber threats, necessitating advanced AI-driven solutions to effectively protect digital identities. This article explores the transformative impact of AI on identity management within the cybersecurity field, focusing on its benefits, challenges, and future potential. A comprehensive review of current literature and empirical findings was conducted, analyzing the application of AI through machine learning, deep learning, and neural networks. The results highlight AI's capability to enable real-time anomaly detection, proactive defense mechanisms, and enhance the resilience of identity protection systems. AI-powered systems exhibit significant advantages in adapting to evolving security threats by providing real-time analysis and understanding the contextual nuances of user behavior. These systems effectively mitigate risks associated with unauthorized access, thereby strengthening overall cybersecurity posture. Key findings emphasize AI's continuous learning from emerging attack tactics, its role in the interpretability of security incidents, and the importance of collaborative frameworks between AI systems and human experts. Addressing challenges such as ethical considerations, algorithmic biases, and the need for transparency remains critical for the ethical deployment and successful integration of AI in cybersecurity.**

***Index Terms*—Artificial Intelligence (AI), Cyber Security, Data Protection, Identity Management, Threat Detection.**

I. Page Layout

THE FIELD of Cyber Security has seen a substantial transition with the introduction of Artificial Intelligence (AI), particularly in the vital areas of Account Takeover (ATO) prevention and Identity Management [1]. It might be difficult for traditional security measures to keep up with the more sophisticated attackers due to the constantly shifting landscape of cyber threats [2]. The field of artificial intelligence has evolved as a transformative instrument, offering sophisticated capabilities to promptly detect, avert, and mitigate identity-related risks [3]. Artificial intelligence (AI)-powered systems can safeguard digital identities and prevent unauthorized access through machine learning algorithms, behavioral analytics, and anomaly detection, among other methods [4]. This article explores the revolutionary effects of AI on identity management, outlining the technology's main benefits, drawbacks, and potential applications in the constantly changing field of cybersecurity [5].

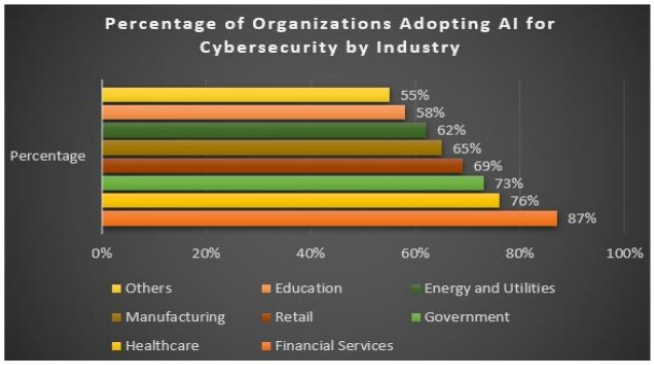

Figure I. Adoption of AI in Cybersecurity by Industry

II. Literature Review

- Camacho (2024) outlined the applications of AI in cybersecurity, including threat detection, vulnerability assessment, incident response, and predictive analysis. Artificial intelligence (AI) systems quickly analyzed enormous amounts of data to find unusual patterns suggestive of possible security breaches by utilizing machine learning techniques. Furthermore, proactive defense mechanisms were made possible by AI-driven technology, giving organizations the ability to proactively minimize risks and protect sensitive information. But the use of AI in cybersecurity also brought up important privacy and ethical issues, so its application must be approached with balance. After conducting a thorough analysis, Camacho emphasized how cybersecurity frameworks must include artificial intelligence (AI) in order to successfully mitigate threats in the digital age [17].
- Varney (2019) examined how artificial intelligence (AI) changed cybersecurity and safeguarded digital ecosystems, pointing out that AI performed better on cognitive tasks than humans, allowing for more complex attacks. The study made clear the necessity of continuing research to improve defenses against threats like malware and phishing that are

enabled by AI. It also covered the unethical differences in AI application between the US and its enemies. Expert systems have been proposed as a way to use AI's ability to identify patterns for defense.

- Chakraborty et al. (2023) talked about how the digital era's technical advancements automated daily tasks but lacked adequate security. They emphasized how difficult it is becoming to secure connected devices and how sophisticated AI-driven cyberthreats are becoming more prevalent. The authors looked at both traditional and sophisticated defense strategies against cyberattacks before offering some possible future uses for AI in cybersecurity.
- Mohammed (2020) talked about how AI may be used to solve cybersecurity problems while highlighting the risks associated with the digital revolution, like data mining and exploitation. It emphasized the value of managing digital identities as well as the possibilities of blockchain technology. In order to combat cybercrime, the report emphasized the necessity for more secure data storage techniques and the shortcomings of conventional systems. Lastly, it discussed how AI may help reduce cyberattacks and solve cybersecurity issues.
- Ansari et al. (2022) explored the use of artificial intelligence (AI) in cybersecurity, emphasizing the technology's expanding impact on the sector. They observed that, as information technology becomes more prevalent in enterprises, cybersecurity is becoming more and more important in the technology sector. The study covered how artificial intelligence (AI) has greatly impacted cybersecurity and how this has resulted in the notable inclusion of machine learning in new cybersecurity-related technologies. In order to examine the overall effects of artificial intelligence on cybersecurity, the writers reviewed the literature, examining both the advantages and disadvantages of the technology.

III. AI In identity management

The role of AI in securing digital identities

Artificial intelligence plays a crucial role in preserving the security of digital identities through the application of state-of-the-art techniques such as machine learning, deep learning, and neural networks [18]. Artificial intelligence (AI) systems possess the capacity to scrutinize copious amounts of data, encompassing user behavior patterns, gadget fingerprints, and contextual details, with the aim of constructing a comprehensive comprehension of every individual's digital identity [6]. Artificial intelligence (AI) can detect anomalies or unauthorized access attempts quickly by establishing a typical user behavior, which can help detect potential security breaches promptly [7].

Understanding contextual nuances and user behavior

AI systems are very good at understanding the nuances and complexity of human behavior, which is essential for identity management to work. By examining user activities such as device usage, network activity, and login times, AI may get a thorough grasp of each user's unique behavioral signature [8]. AI can distinguish between legitimate user behaviors and suspect activity thanks to this contextual understanding, even in situations where the latter may resemble the former quite a bit .

Real-time anomaly detection

The capacity of AI to detect anomalies in real-time is one of its primary benefits for identity management. AI systems monitor user behavior continuously, contrasting it with known threat patterns and behavioral baselines [9]. AI has the ability to detect anomalies, such as an odd login location or an abrupt shift in user behavior, and to set off pre-established security protocols and generate notifications. Preventing unwanted access and lessening the effects of any security breaches require the capacity to detect in real time.

Proactive defense against unauthorized access attempts

AI makes it possible to defend against unwanted access attempts in a proactive manner. Artificial intelligence (AI) can remain one step ahead of prospective adversaries by constantly learning and adapting to shifting danger scenarios. Security systems can proactively take preventive action by using machine learning algorithms that are able to recognize trends and indicators that could indicate possible threats. Furthermore, AI can automate the application of security guidelines and access restrictions, ensuring that only those with permission can access confidential information [10].

A. AI in Account Takeover (ATO) Prevention

Figure 2. Percentage of Successful Cyber Attacks Prevented by AI-based Security Systems

B. Recognizing patterns indicative of compromised accounts

The detection of patterns that indicate compromised accounts is a critical function of artificial intelligence, which aids in the prevention of Account Takeover (ATO). Large amounts of data, including login attempts, user behavior,

and device information, can be analyzed by machine learning algorithms to find potentially suspicious activity [11]. AI, for example, can detect unusual login locations, sudden changes in a user's behavior, or multiple failed attempts at authentication, all of which could be signs of an account compromise. When these trends are identified in a timely manner, AI-powered systems can initiate alerts and quickly take corrective action, like freezing an account or adding further verification processes.

C. Employing multi-factor authentication

The effectiveness of multi-factor authentication (MFA) in preventing unwanted access is greatly increased by AI. Conventional MFA relies on inflexible guidelines and preset challenges that proficient attackers can easily circumvent. In contrast, MFA that is powered by AI dynamically modifies authentication difficulties according to environmental circumstances and the user's risk profile [12]. For instance, AI may request additional authentication information from the user, such as biometric data or a one-time password, if it detects a login attempt from an unknown device or location. Organizations can utilise risk-based authentication with AI, enabling the deployment of the appropriate level of security in response to the perceived threat level [19].

D. Continuous learning from evolving attack tactics

AI gives security systems the ability to predict changing attack strategies and react continuously, keeping them one step ahead of their enemies. Cybercriminals are constantly coming up with new techniques to launch ATO attacks, such as social engineering, credential stuffing, and phishing. Artificial intelligence (AI)-enabled systems can learn from changing strategies by analyzing past attack data, seeing new trends, and then updating their algorithms. Organizations are able to maintain a robust defense against attempts to obtain unauthorized access and respond to evolving risks thanks to this continuous learning process. AI can also detect any security flaws in the system and recommend improvements to make it more secure overall.

E. Enhancing the resilience of identity protection mechanisms

By providing an additional layer of security, artificial intelligence fortifies the resilience of identity protection systems. Passwords and security questions are examples of traditional identity protection techniques that are commonly vulnerable to social engineering and brute-force attacks. By applying cutting-edge methods like behavioral biometrics and user profiling, AI can improve these mechanisms. To create a unique behavioral signature, AI, for example, might examine a variety of inputs, including mouse movements, typing habits, and device interactions. Along with more traditional authentication techniques, this signature can be used to confirm the user's identity. By combining artificial intelligence (AI) with well-established identity protection protocols, businesses may create a strong, adaptable security framework that effectively thwarts efforts by unauthorized individuals to gain access [21].

IV. Advantages of AI in Identity Management

TABLE I. Advantages of AI in Identity Management

Advantage	Description
Adaptability to evolving security tactics	AI algorithms can quickly learn and adapt to new security threats, ensuring that the system remains effective against the latest attack tactics.
Providing interpretable insights	AI-powered systems offer interpretable insights into security incidents, enabling security teams to understand the underlying causes and take appropriate actions.
Real-time analysis for efficient response	AI enables real-time analysis of identity-related data, facilitating efficient response mechanisms to security incidents and minimizing the potential impact [20].
Understanding contextual nuances	AI excels at understanding contextual nuances and learning from diverse cyber scenarios, enhancing its effectiveness in identifying and mitigating identity-related risks.
Proactive defense against emerging threats	AI enables a proactive defense against emerging threats by continuously monitoring user behavior and system activity, allowing organizations to take preventive measures.
Mitigating risks and safeguarding sensitive data	AI plays a crucial role in mitigating risks and safeguarding sensitive information by implementing robust access controls, monitoring mechanisms, and detecting anomalous activities.

A. Adaptability to evolving security tactics

Because AI is so flexible, it provides a huge advantage in identity management when it comes to adjusting to evolving security strategies. Artificial intelligence (AI) has the capacity to pick up on changes in cybercrimes' tactics swiftly, as they are constantly evolving [13]. AI algorithms may automatically update their threat detection models by analyzing large volumes of data and spotting new trends, which keeps the security system up to date against the most modern dangers. To stay ahead of opponents and keep up a strong defense against identity-related attacks, one must be flexible.

B. Providing interpretable insights into security incidents

Identity management systems driven by artificial intelligence (AI) offer insightful information about security events, enabling security teams to comprehend the type and source of risks. AI is capable of producing in-depth reports and visualizations that offer thorough justifications for the

choices it makes. These revelations may include the particular behavior information offered includes the precise patterns of behaviour or abnormalities that set off an alarm, the sequence of events that preceded the incident, and the possible effects on the organisations. Security teams are capable of prioritising response actions, making well-informed judgements, and successfully reducing risks [14].

C. Real-time analysis for efficient response mechanisms

AI makes it possible to analyse identity-related data quickly, which facilitates the development of efficient reaction plans for security events [22]. AI is capable of identifying abnormalities and possible threats in real-time by utilising its enormous data processing capabilities. Security teams may act quickly by blocking bogus login attempts, isolating affected accounts, or triggering incident response procedures thanks to this real-time analysis. AI is essential in decreasing the possible impact of identity-related attacks and helping organisations maintain the integrity of their systems by shortening the time lag between threat detection and reaction.

D. Understanding contextual nuances and learning from diverse cyber scenarios

AI exhibits a great capacity to learn from a variety of cyber scenarios and grasp the complex intricacies of identity management. AI has the capacity to generate comprehensive profiles of both common and uncommon actions by analysing a variety of data points, including user behaviour, device information, and network activity. AI can differentiate between legitimate user behaviours and possible dangers even in situations where the differences are subtle because of its contextual understanding [15]. Furthermore, AI continuously improves its algorithms and gains accuracy over time by learning from a variety of cyber scenarios it encounters. AI is a powerful tool for identifying and reducing identity-related hazards because of its ability to understand context and learn from experience.

E. Proactive defense against emerging threats

AI strengthens identity management's proactive defence against new threats [16]. AI can identify possible weaknesses and weak points in the security posture by continuously monitoring user behaviour and system activity. Businesses that adopt a proactive approach may be able to patch security flaws before hackers can exploit them. AI can also assess the effectiveness of existing security measures and simulate different attack scenarios, which helps organisations find and fix weaknesses in their identity management systems [23]. Organisations can keep ahead of adversaries and lower the likelihood of successful identity-related attacks by implementing a proactive approach with AI.

F. Mitigating risks and safeguarding sensitive information

In identity management, artificial intelligence (AI) is essential for reducing risks and safeguarding sensitive data. Artificial Intelligence successfully lowers the risk of unauthorised access, data breaches, and identity theft by accurate identification and quick reaction to possible threats. Strict access controls can be enforced with the use of AI-powered solutions, ensuring that only authorised users have access to sensitive resources [24]. Furthermore, AI can keep an eye on user behaviour and spot any potentially worrying activities, such unusual data access patterns or attempts to harvest private information. AI helps organisations protect their most important assets and maintain the security, dependability, and accessibility of sensitive data by notifying security staff in a timely manner and putting preventive steps in place [25].

V. Challenges and Considerations

Machine learning and deep learning algorithms are used by cybersecurity experts to perform tasks like intrusion detection, malware analysis, and anomaly identification. Every algorithm has pros and cons of its own, and the best approach relies on the particular security problem that needs to be solved. Here are a few instances of outcomes from various algorithms:

- *Support Vector Machines (SVM):* SVM is a popular intrusion detection technique that has proven to be effective at recognising known attacks. For example, SVM was used in conjunction with ant colony networks in a study by Feng et al. to detect network invasions. Using the KDD Cup 1999 dataset, the study attained an outstanding accuracy rate of 96.75%.
- *Deep Learning:* Deep learning methods such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) have demonstrated promising outcomes in identifying intricate and unfamiliar attacks. Jiang et al. demonstrated a multichannel CNN in their work that was able to identify clever attacks with remarkable accuracy—99.98% —on the NSL-KDD dataset. CNN and RNN were combined to create a deep learning method for network intrusion detection by Shone et al. Their accuracy on the KDD Cup 1999 dataset was 97.85%.
- *Ensemble Methods:* Several learning techniques combined improve robustness and speed. Xin et al. integrated deep belief networks (DBN) and support vector machines (SVM) to efficiently detect intrusions. They achieved an amazing accuracy rate of 99.14% on the NSL-KDD dataset [26].
- *Transfer Learning:* Utilising expertise from one field to improve performance in another. Transfer learning is effective in detecting new attack patterns, as demonstrated by Gu et al. who used it to find weaknesses in the supply chain of the machine learning model [27].
- *Sequential Models:* Because sequential models are so good at modeling sequential data, they have been used extensively to identify IoT-botnet attacks. One example of this is Long Short-Term

Memory (LSTM) networks. On a customised dataset, the LSTM-based method suggested by Soe et al. effectively identified IoT-botnet attacks with an astounding accuracy of 99.23% [28].

These findings demonstrate how various algorithms perform differently in some cybersecurity tasks. It's crucial to recognise the difficulties and restrictions associated with any method, though. These include the need for large-scale datasets that have been annotated, the potential for adversarial attacks, and the models' interpretability. Taking into account the unique requirements and constraints of respective cybersecurity applications, researchers and practitioners should carefully evaluate the suitability of different algorithms [29].

TABLE II. CHALLENGES AND CONSIDERATIONS IN IMPLEMENTING AI FOR CYBERSECURITY

Challenge/ Consideration	Description
Ensuring the ethical use of AI	Organizations must establish clear guidelines and protocols to govern the collection, storage, and analysis of data used by AI systems, ensuring alignment with ethical principles and individual privacy rights.
Addressing potential biases in AI algorithms	To mitigate biases, organizations must ensure that the training data is diverse, representative, and free from discriminatory patterns, and regularly audit and test AI algorithms for fairness.
Maintaining transparency and accountability	Organizations should strive for explainable AI, where the reasoning behind AI decisions is clearly articulated, and establish accountability mechanisms, such as regular audits and oversight committees, to ensure responsible use of AI systems.
Collaborating with human experts	Effective collaboration between AI systems and human experts is essential for achieving optimal results, leveraging the strengths of both artificial and human intelligence to develop a comprehensive approach to cybersecurity.

A. Ensuring the ethical use of AI in Cyber Security

As AI grows more common in cybersecurity, ethical use becomes harder. AI systems may analyze massive amounts of sensitive data, raising privacy and abuse concerns. Clear policies and processes are needed to regulate AI data collection, storage, and processing. AI systems must also be responsible, open, and just. To maintain trust and avoid unanticipated consequences, AI systems must prioritize person rights and respect the law and ethics.

B. Addressing potential biases in AI algorithms

AI biases must be addressed in cybersecurity. When AI systems learn algorithms from biased data in the training set, biases may be reinforced. An AI system trained on a dataset of attacks from a given demographic may become biased in identifying threats from that demographic. This can cause false positives and unjust profiling. To reduce preconceptions, organizations must prioritize diverse, representative training data without bias. Audits and testing must be done often to discover and fix bias-related issues.

C. Maintaining transparency and accountability

Accountability and transparency are essential when employing AI in cybersecurity. AI systems' complicated and confusing decision-making mechanisms might make decisions hard for stakeholders to understand. AI-powered security systems without transparency may lose trust and raise issues about their impartiality. To solve this problem, organizations should aim toward explainable AI, which explains AI judgments to humans. Additionally, oversight committees and frequent audits can help ensure that AI systems are working as planned and meeting organizational and legal standards.

D. Collaborating with human experts for optimal results

AI in cybersecurity requires human involvement for optimum results. Despite their proficiency at processing huge volumes of data and spotting hidden patterns, AI algorithms are worse at contextual comprehension and intuition than humans [30]. Analysts must understand the security environment, analyze AI algorithm outputs, and make informed recommendations. Collaboration between artificial and human intelligence can boost cybersecurity [31]. Organizations must encourage cooperation and give training to integrate AI technology into security operations [32-25].

VI. FUTURE DIRECTIONS

A. Continuous advancements in AI technologies for Cyber Security

AI technology is improving cybersecurity and driving innovation. AI algorithms should improve our ability to solve complicated cybersecurity problems. Deep learning methods like generative adversarial networks (GANs) can provide more varied and realistic datasets to help AI models recognize and respond to new threats [22]. Advances in sentiment analysis and natural language processing (NLP) may allow AI systems to better interpret unstructured data like social media and forum postings to identify security issues. Advancements in AI technologies are expected to defend organizations against cyber-attacks.

B. Integration of AI with other emerging technologies (e.g., blockchain, quantum computing)

AI in cybersecurity may take an interesting turn when combined with blockchain and quantum computers. These technologies enable organizations to build resilient systems that can handle today's complicated threat scenario. Blockchain technology can securely log security issues and protect AI model training data. Quantum computing could improve traditional computer systems by helping AI algorithms detect and respond to threats faster. As AI and cybersecurity technologies advance, we may expect new and inventive uses.

C. Fostering interdisciplinary research and collaboration

Interdisciplinary research and collaboration are needed to maximize AI's cybersecurity potential. Cybersecurity is complex and requires knowledge in computer science, mathematics, psychology, and social science. Collaboration between scholars and practitioners from diverse fields can improve cybersecurity. This strategy considers complicated organizational-human connections that determine cyber risk. This may encompass interdisciplinary research centers and programs and opportunities for industry, government, and academia to collaborate and share knowledge. By combining stakeholders' perspectives and expertise, we can build a more secure digital future.

VII. Conclusion

In conclusion, the integration of artificial intelligence (AI) into cybersecurity has brought about significant transformations in identity management and threat detection. AI-powered systems offer unparalleled capabilities in securing digital identities, detecting anomalies, and preventing unauthorized access attempts through advanced machine learning algorithms and real-time analysis. Moreover, AI enables proactive defense mechanisms, continuous learning from evolving attack tactics, and the enhancement of resilience in identity protection mechanisms. Despite these advantages, challenges such as ensuring ethical use, addressing biases in AI algorithms, maintaining transparency and accountability, and collaborating effectively with human experts must be carefully considered and addressed.

Looking ahead, the future of AI in cybersecurity holds immense potential for further advancements. Continuous improvements in AI technologies are expected to enhance our ability to address complex cybersecurity issues, while integration with other emerging technologies like blockchain and quantum computing promises to create stronger and more resilient cybersecurity systems. Fostering interdisciplinary research and collaboration will be crucial in fully realizing AI's potential in cybersecurity, as it requires expertise from various fields to tackle the multidimensional nature of cyber risk effectively. By leveraging AI technologies and fostering collaboration across disciplines, we can pave the way for a more robust and secure digital future

References

[1] Benhadjyoussef, N., Karmani, M., & Machhout, M. (2021). Power-based Side Channel Analysis and Fault Injection: Hacking Techniques and Combined Countermeasure. International Journal of Advanced Computer Science and Applications, 12(5).

[2] Babu, V. H., & Balaji, K. (2020). Survey on modular multilevel inverter based on various switching modules for harmonic elimination. In Intelligent Computing in Engineering: Select Proceedings of RICE 2019 (pp. 451-458). Springer Singapore.

[3] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7, 1-29.

[4] Arri, H. S., Singh, R., Jha, S., Prashar, D., Joshi, G. P., & Doo, I. C. (2021). Optimized task group aggregation-based overflow handling on fog computing environment using neural computing. *Mathematics, 9*(19), 2522. https://doi.org/10.3390/math9192522

[5] Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2021). Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR), 54(5), 1-36.

[6] Wang, Z., Wang, E., & Zhu, Y. (2020). Image segmentation evaluation: a survey of methods. Artificial Intelligence Review, 53(8), 5637-5674.

[7] Jha, S., Ahmad, S., Arya, A., Alouffi, B., Alharbi, A., Alharbi, M., & Singh, S. (2023). Ensemble learning-based hybrid segmentation of mammographic images for breast cancer risk prediction using fuzzy C-means and CNN model. *Journal of Healthcare Engineering, 2023*(1), 1491955. https://doi.org/10.1155/2023/1491955

[8] Camacho, N. G. (2024). The role of ai in cybersecurity: Addressing threats in the digital age. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 3(1), 143-154.

[9] Varney, A. (2019). Analysis of the impact of artificial intelligence to cybersecurity and protected digital ecosystems (Master's thesis, Utica College).

[10] Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial intelligence for cybersecurity: Threats, attacks and mitigation. In Artificial Intelligence for Societal Issues (pp. 3-25). Cham: Springer International Publishing.

[11] Mohammed, I. A. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. Artif. Intell, 7(9), 1-5.

[12] Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: a literature review. International Journal of Advanced Research in Computer and Communication Engineering.

[13] Jha, S., Jha, N., Prashar, D., Ahmad, S., Alouffi, B., & Alharbi, A. (2022). Integrated IoT-based secure and efficient key management framework using hashgraphs for autonomous vehicles to ensure road safety. *Sensors, 22*(7), 2529. https://doi.org/10.3390/s22072529

[14] Sharma et al., "Artificial Intelligence Techniques for Landslides Prediction Using Satellite Imagery," in IEEE Access, vol. 12, pp. 117318-117334, 2024

[15] Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176.

[16] Jha, S., Kumar, R., Hoang Son, L., Abdel-Basset, M., Priyadarshini, I., Sharma, R., & Viet Long, H. (2019). Deep learning approach for software maintainability metrics prediction. *IEEE Access, 7,* 61840–61855. https://doi.org/10.1109/ACCESS.2019.2913349

[17] Feng, W., Zhang, Q., Hu, G., & Huang, J. X. (2014). Mining network data for intrusion detection through combining SVMs with ant colony networks. Future Generation Computer Systems, 37, 127-140.

[18] Jiang, F., Fu, Y., Gupta, B. B., Liang, Y., Rho, S., Lou, F., ... & Tian, Z. (2018). Deep learning based multi-channel intelligent attack detection for data security. IEEE transactions on Sustainable Computing, 5(2), 204-212.

[19] Ahmad, S., Jha, S., Eljialy, A. E. M., & Khan, S. (2021). A systematic review on e-wastage frameworks. *International Journal of Advanced Computer Science and Applications, 12*(12). https://doi.org/10.14569/IJACSA.2021.0121287

[20] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE transactions on emerging topics in computational intelligence, 2(1), 41-50.

[21] Rajagopal, S. Ahmad, S. Jha, H. A. M. Abdeljaber, and J. Nazeer, "AI Based Secure Analytics of Clinical Data in Cloud Environment: To-

wards Smart Cities and Healthcare," J. Adv. Inf. Technol., vol. 14, no. 5, pp. 1132-1142, 2023.

[22] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. Ieee access, 6, 35365-35381.

[23] Jha, S., Nkenyereye, L., Prasad Joshi, G., & Yang, E. (2020). Mitigating and monitoring smart city using internet of things. *Computers, Materials & Continua, 65*(2), 1059–1079. https://doi.org/10.32604/cmc.2020.011754

[24] Gu, T., Dolan-Gavitt, B., & Garg, S. (2017). Badnets: Identifying vulnerabilities in the machine learning model supply chain. arXiv preprint arXiv:1708.06733.

[25] Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2020). Machine learning-based IoT-botnet attack detection with sequential architecture. Sensors, 20(16), 4372.

[26] Jha, S., Prasad Joshi, G., Nkenyereya, L., Wan Kim, D., & Smarandache, F. (2020). A direct data-cluster analysis method based on neutrosophic set implication. *Computers, Materials & Continua, 65*(2), 1203–1220. https://doi.org/10.32604/cmc.2020.011618

[27] Jha, S., Prashar, D., Long, H. V., & Taniar, D. (2020). Recurrent neural network for detecting malware. *Computers & Security, 99,* 102037. https://doi.org/10.1016/j.cose.2020.102037

[28] Saad, A., Faddel, S., Youssef, T., & Mohammed, O. A. (2020). On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber-attacks. IEEE transactions on smart grid, 11(6), 5138-5150.

[29] Jha, S., Seo, C., Yang, E., & Joshi, G. P. (2021). Real-time object detection and tracking system for video surveillance. *Multimedia Tools and Applications, 80*(3), 3981–3996. https://doi.org/10.1007/s11042-020-09749-x

[30] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. IEEE access, 8, 222310-222354.

[31] Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K. L. A., Elkhatib, Y., ... & Al-Fuqaha, A. (2019). Unsupervised machine learning for networking: Techniques, applications and research challenges. IEEE access, 7, 65579-65615.

[32] S. Jha, S. Routray, H. A. M. Abdeljaber, and S. Ahmad, "A novel approach for decision support system in cricket using machine learning," Int. J. Comput. Appl. Technol., vol. 70, no. 2/3, pp. 86-92, 2022.

[33] Xiao, L., Wan, X., Dai, C., Du, X., Chen, X., & Guizani, M. (2018). Security in mobile edge caching with reinforcement learning. IEEE Wireless Communications, 25(3), 116-122.

[34] S. Jha, "Model Selection Procedure in Alleviating Drawbacks of The Electronic Whiteboard," 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2021, pp. 319-322

[35] V. Puri et al., "A Hybrid Artificial Intelligence and Internet of Things Model for Generation of Renewable Resource of Energy," in IEEE Access, vol. 7, pp. 111181-111191, 2019