JOURNAL OF ENGINEERING, EMERGING TECHNOLOGIES AND APPLIED SCIENCES (JEETAS)

A PUBLICATION OF THE FACULTY OF ENGINEERING, NIGER DELTA UNIVERSITY

NOVEMBER 2023 VOLUME 01 ISSUE 02 ISSN: 1116 - 4514

ARTICLES

- A message From the Editor-in-Chief — i
  Z. R. Yelebe
- Bioremediation of Crude Oil PollutedSoil Using a Blend of NPK Fertilizer and Periwinkle Shell Ash — 1 - 8
  B. Z. Yelebe and Z. R. Yelebe
- Recycling of Waste Engine Oil using Acetic and Lactic Acids as Washing Agents — 9 - 17
  O. Ketebu, E. Komonibo, and E. M. Gbafade
- Niger Delta University Campus Borehole Water Quality Analysis for Domestic Purposes: Treated Versus Raw Water. — 18 - 26
  R. K. Douglas, E. Komonibo, and A. W. Opukumo
- Reducing Pipeline Corrosion in Oil and Gas Industries Using Ant Colony Optimization Techniques Agents — 27 - 33
  E. O. Ikpaikpai and J. Eke
- Assessment of Stress-Strain Behaviour of Sea Sand Sandcrete Blockwalls with Different Mix Ratio — 34 - 40
  D. A. Wenapere and T. S. Orumu
- Microgrid Congestion Management Using Swarm Intelligence Algorithm — 41 - 48
  A. U. Emmanuel and A. F. James
- Determinationof Carbon Dioxide (CO2) Emissions from Perkins P220-3 AGO-Based Generating Plant in Variable Temperature and Relative Humidity — 49- 55
  S. Adianimovie
- Analysis of Electromagnetic Wave Propagation in Human Tissue — 56 - 67
  G. Biowei, S. A. Adekola, and A. K. Benjamin
- Model Development for Prediction of Concrete Compressive Strength: Advancing Construction Industry Practices and Quality Control Standards — 68 - 75
  J. A. TrustGod, D. A. Wenapere, J. Odudu, and S. A, Appi
- Strength Properties of Paving Stone Composites with Polyethylene Terephthalate (PET) as Total Cement Replacement — 76 - 81
  E. Kiridi, D. H. Mac-Eteli, and B. M. Alagba
- Soxhlet Extraction of Oil from Monkey Sugarcane (Costus afer) Leaves — 82 - 87
  B. E. Yabefa, W. Burubai, and B. J. Jonathan
- Application of Artificial Intelligence (AI) Model to Mitigate Security threats of Internet of Things (IoT) : A Review — 88 - 96
  S. M. Ekolama and D. Ebregbe
- Relay Coordination for Efficient PowerDelivery and Equipment Protection at StationRoad, Port-Harcourt — 97 - 104
  A. K. Benjamin and N. W. Aguiyi
- Absorbed Dose Rate of Some Body Organs in Diete-Koki Memorial Hospital, Opolo, Yenagoa, Bayelsa State — 105 - 110
  G. E. Ogobiri, I. E. Abule, K. E. Dauseye,and U. P. Amanuche
- Advancements in Autonomous Battery Monitoring: A System with Auto-Return Home Integration — 111 - 117
  F. O. Agonga J. C. Anunuso,B. Alkali, M. S. Abubakar, and C. T. Ikwouazom
- Optimization of Power Generation in South-South, Nigeria Using Leap Model — 118 - 128
  A. A. Dada, P. K. Ainah and A. O. Ibe

NIGER DELTA UNIVERSITY

Journal of Engineering, Emerging Technologies and Applied Sciences -– Volume 1 Issue 2, Nov. 2023

Available at ***https://www.ndu.edu.ng/journalofengineering/***

RESEARCH ARTICLE OPEN ACCESS

Application of Artificial Intelligence (AI) Model to Mitigate Security threats of Internet of Things (IoT): A Review

*Solomon Malcolm Ekolama, **David Ebregbe

*Department of Agricultural and Environmental Engineering, Niger Delta University, Bayelsa State, Nigeria

**Department of Electrical and Electronic Engineering, Niger Delta University, Bayelsa State, Nigeria

solomon.ekolama@ndu.edu.ng

----------**********----------

Abstract:

The convergence of the Internet of Things (IoT) and Artificial Intelligence (AI) is transforming data and technology exchange across a number of industries, including smart cities, transportation, healthcare, and agriculture. Adoption of IoT has transformed many industries, but it has also sparked worries about security flaws in network integrity, authentication, and data privacy. AI models have proven to be a pro-active and successful means to deal with these security issues in IoT networks. AI-based solutions are essential to mitigate security risks in Internet of Things settings because they include advanced features like behaviour analysis, anomaly identification, and threat prediction. This artificial intelligence (AI)-driven solutions improve behaviour analysis, anomaly detection, and real-time threat detection, protecting networks against cyberattacks and guaranteeing data security, privacy, and confidentiality. To maximise the benefits of AI in mitigating IoT security issues and fostering confidence in IoT technology, future efforts should concentrate on overcoming current limitations and challenges in AI for IoT security, exploring potential developments and research directions, and addressing ethical and regulatory considerations.

Keywords **— Internet of Things (IoT), Cyberattack, Artificial Intelligence (AI), Security threats, Authentication, Data privacy, Network integrity, Anomaly Detection, Predictive Analytics, Machine Learning Algorithms, Intrusion Detection Systems (IDS).**

----------**********----------

I. INTRODUCTION

The integration of Artificial Intelligence (AI) and the Internet of Things (IoT) is fundamentally changing the way we interact with data and technology, transforming sectors like healthcare, transportation, agriculture, and smart cities (Alahi et al., 2023). However, the widespread adoption of IoT has raised security concerns, including vulnerabilities in authentication, data privacy, and network integrity (Chanal & Kakkasageri, 2020). The use of AI models to mitigate these issues has gained prominence as a proactive and effective approach to addressing these security issues in IoT ecosystems (Malhotra et al., 2012).

A network of interconnected devices, sensors, and systems that exchange information and communicate via the internet constitutes the Internet of Things (IoT). For the purposes of real-time monitoring, predictive analytics, and automated decision-making, it has produced enormous quantities of data. Nevertheless, IoT devices are susceptible to cyber threats such as denial-of-service attacks, unauthorised access, and data intrusions due to their interconnectedness.

Models based on artificial intelligence (AI) are indispensable for mitigating security threats in IoT environments (Zaman et al., 2021). They provide sophisticated functionalities such as the ability to detect anomalies, analyse behaviour, and predict threats. Machine learning algorithms are capable of

analysing immense amounts of data, detecting anomalous patterns, and mitigating cyber threats in real time (Inuwa & Das, 2024). In addition to bolstering the resilience of IoT ecosystems, authentication mechanisms, access control policies, and encryption techniques powered by AI ensure the integrity of data and the reliability of systems.

II. ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Artificial intelligence (AI) is playing a crucial role in the Internet of Things (IoT) by improving threat identification, anomaly detection, and predictive analytics as shown in Figure 1.

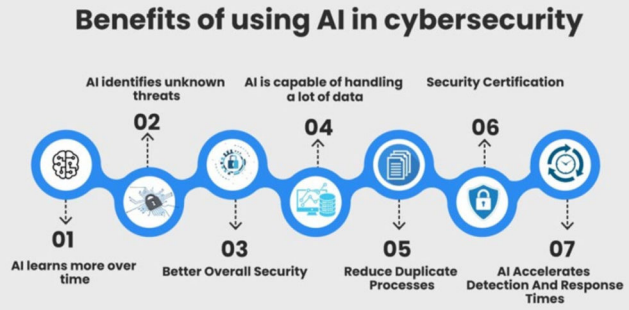

Figure 1: AI in Cyber Security and IoT. (Source: Augmented AI, 2023)

As shown in Figure 1, AI systems use machine learning methods like reinforcement learning, supervised learning, and unsupervised learning to analyse large data volumes, identify security risks, monitor network traffic, flag suspicious activity, and trigger automatic responses to combat cyberattacks. AI-driven authentication and encryption systems ensure the confidentiality, availability, and integrity of sensitive information.

Artificial intelligence (AI) is increasingly crucial in protecting data on the Internet of Things (IoT). AI uses behaviour analysis, threat detection, and automatic response mechanisms to enhance cybersecurity. Machine learning algorithms help identify patterns, outliers, and security breaches in large amounts of data. AI also enhances privacy, secrecy, and security through authentication systems, encryption technologies, and access control rules.

Artificial intelligence (AI) is playing a crucial role in cybersecurity in IoT settings by providing real-time threat detection, anomaly detection, and behaviour analysis. Intrusion detection systems (IDS) protect networks from cyberattacks by monitoring traffic and identifying suspicious behaviors. AI-driven authentication methods, encryption techniques, and access control rules enhance data security, privacy, and confidentiality. AI-powered predictive analytics and threat intelligence help firms anticipate potential dangers and strengthen their security in the evolving IoT environment.

III. SECURITY THREATS OF IOT DEVICES: CHALLENGES AND AI SOLUTIONS

Enhancing security resilience of IoT ecosystems can be achieved through the implementation of Artificial Intelligence (AI) models that perform proactive threat detection, anomaly identification, and automated response mechanisms. This can effectively mitigate the security risks associated with IoT devices, such as unauthorised access and data breaches as shown in Figure 2.

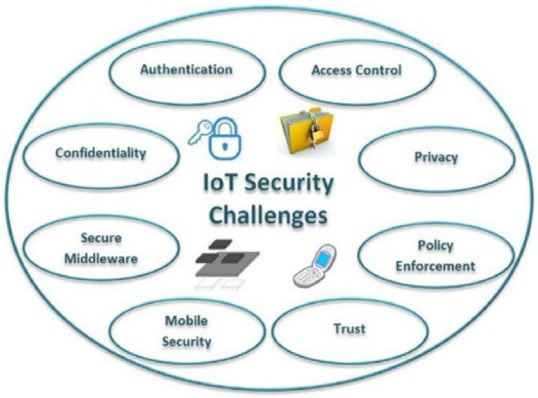

Figure 2: Security Challenges of IoT (Source: Torğul et al., 2016)

The following are some areas of security concerns shown in Figure 2 and suggested solutions using artificial intelligence:

A. Weak Authentication and Authorization

Challenges: IoT devices pose security risks due to flaws in authorization and authentication protocols, allowing unauthorised access and credential theft (Tawalbeh et al., 2020). Insufficient authorization mechanisms can lead to breaches and data compromises. The fragmented and decentralised structure of IoT ecosystems complicates these issues.

Solution: AI-based access control and authentication can be employed to improve security on IoT devices by reducing flaws in traditional systems. AI algorithms also minimise unauthorised access and credential theft, enabling authentic permission management based on user behaviour and risk assessment scores (Wu et al., 2020). AI also ensures Real-time monitoring of suspicious activity and potential breaches improves security. Integrating AI increases resilience and protects IoT ecosystems from evolving cyber threats.

B. Insecure Network Connections

Challenges: IoT devices with insecure network connections run the risk of serious security breaches due to data interception, man-in-the-middle attacks, and eavesdropping (Hasan et al., 2022). Because of shoddy authentication procedures, poor encryption techniques, or incorrectly configured network settings, these vulnerabilities are susceptible to malevolent actors' exploits. Strong encryption standards, safe communication protocols, frequent security audits, and network traffic monitoring are required for IoT device protection.

Solution: AI-driven network security solutions protect IoT devices from security threats, especially insecure connections. By continuously monitoring and analysing network traffic patterns, AI algorithms detect anomalies, potential threats, and data breaches (Abed & Anupam, 2023). Real-time intrusion detection systems respond to suspicious activities, while encryption and authentication mechanisms ensure data confidentiality. Machine learning algorithms adapt to evolving attack vectors.

C. Lack of Firmware Updates

Challenges: IoT devices without firmware upgrades pose security and operational risks due to potential vulnerabilities that can allow hackers to steal data or conduct cyberattacks (Djenna et al., 2021). Frequent updates deprive devices of crucial security patches, bug fixes, and performance improvements, making it challenging to adapt to changing threats and maintain peak efficiency. Proactive measures like secure update systems, vendor cooperation, and user education are necessary.

Solution: By examining firmware code, finding vulnerabilities, and ranking security fixes, AI-powered firmware security and vulnerability management may assist IoT devices in addressing security threats. Firmware integrity is ensured by machine learning techniques that can identify unusual behaviour in firmware upgrades. Predictive analytics powered by AI is able to foresee new risks and provide countermeasures (Shrivastwa, 2023). By incorporating AI into firmware security procedures, security resilience is increased, risks related to obsolete firmware are reduced, and ongoing defence against prospective attacks is guaranteed.

D. Data Privacy Concerns

Challenges: The Internet of Things (IoT) faces a significant challenge in terms of data privacy due to inadequate security measures. IoT devices collect vast amounts of sensitive data, such as user behaviour and health information, without safeguards, putting user security and privacy at risk. Comprehensive solutions, including robust encryption protocols, data anonymization methods, access control mechanisms, and privacy-first design principles, can help protect user data.

Solution: Encryption and data privacy strategies powered by artificial intelligence can assist

organisations in addressing privacy concerns in Internet of Things installations. These solutions implement strong encryption methods using AI algorithms, thereby thwarting unauthorised access and data breaches. By analysing user behaviour and data trends, machine learning algorithms can detect privacy issues, allowing for preventative measures such as data anonymisation and differential privacy strategies. Implementing AI-driven strategies improves the resilience of security and data protection measures (Kavitha et al., 2021).

E. Physical Security Risks

Challenges*:* IoT device physical security vulnerabilities present a substantial risk to the integrity of network infrastructure and the protection of data. Physical theft, inadequate device hardening, and the absence of intrusion detection measures are a few examples. These vulnerabilities can be exploited by cybercriminals to acquire sensitive data, compromise the functionality of devices, or obtain unauthorised access (Garagad et al., 2020).

Solution: IoT device security may be greatly improved by using AI-powered physical security measures. AI algorithms are used by sophisticated surveillance systems to instantly identify abnormalities and assess dangers. While machine learning algorithms find new dangers and vulnerabilities in security data, video analytics set off automatic responses and alerts. Authorised personnel may access vital sites and Internet of Things equipment with the help of technologies like biometric identification and AI-driven access control (Awad et al., 2024).

F. Botnets and DDoS Attacks

Challenges*:* The rise of botnets and DDoS attacks on IoT devices poses a significant security challenge due to their numerous vulnerabilities and lack of security measures. These attacks can overload networks and disrupt services. Identifying and preventing botnet attacks is challenging due to the complexity of IoT installations (Salim et al., 2020).

Solution: To mitigate these threats, AI can help organisations mitigate security risks associated with IoT devices, such as botnets and DDoS attacks. AI-driven threat detection systems monitor network traffic and device activity, triggering real-time warnings and automatic reactions. Machine learning algorithms can adapt to changing attack vectors, reducing botnet and DDoS attacks' impact on IoT ecosystems. Integrating AI-driven capabilities strengthens security measures, increases threat visibility, and proactively protects against advanced cyber threats (Chakraborty et al., 2023).

G. Supply Chain Vulnerabilities

Challenges: The security of IoT devices is a complex issue due to the interconnected nature of supply chains, which involve stakeholders like device makers, component suppliers, software developers, and third-party vendors. Vulnerabilities can arise from supply chain attacks, corrupted components, or malicious firmware changes. The global supply chain environment complicates ensuring resilience against cyber-attacks and assessing component security posture (Sobb et al., 2020).

Solution: Artificial intelligence (AI) can improve the security of Internet of Things devices by addressing supply chain vulnerabilities. AI-powered algorithms can evaluate component safety, identify irregularities, and identify potential threats. Real-time monitoring, anomaly detection, and automated reaction mechanisms minimise security risks. Machine learning algorithms can improve cyber resilience by learning from past data and suggesting preventative measures. AI-driven security systems enhance integrity, protect devices from breaches, and improve visibility and accountability, ultimately enhancing trustworthiness in connected ecosystems (Nagaty, 2023).

H. Integration Challenges

Challenges*:* The integration of IoT devices poses significant security risks due to the variety of

devices, protocols, platforms, and settings. Adopting complete security frameworks and consistent procedures is challenging due to compatibility issues, interoperability hurdles, and a lack of standardised protocols (Jurcut et al., 2020).

Solution: AI-powered integration solutions enhance IoT device integration, reducing complexity and human involvement. They automate device identification, setup, and administration, detecting irregularities and security breaches in real-time. These solutions enable proactive threat detection and automatic response mechanisms, centralised monitoring, and the enforcement of security regulations. They enhance interoperability and security resilience, responding to changing IoT settings and ensuring ongoing compliance with security standards (Alahi et al., 2023).

IV. CASE STUDIES AND EXAMPLES

AI-driven solutions enhance IoT ecosystem security by monitoring network traffic, analysing data trends, and triggering automatic responses. They protect sensitive information through authentication, encryption, and access rules, enabling predictive analytics and threat intelligence. This is demonstrated by following case studies:

a. "*Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*"

Fraudsters laundered €220,000 ($243,000) in Europe in March 2019 by assuming the identity of the CEO of a United Kingdom-based energy company. The CEO believed he was discussing with the CEO of his German parent company, who instructed him to transfer the funds within an hour, as shown in figure 3. The organisation's insurance provider, Euler Hermes Group SA, concealed the identities of the victim companies. It is unknown whether this is the first occurrence of an attack of this nature, but law enforcement officials and AI researchers assert that criminals will use AI to automate cyberattacks (Stupp, 2019).

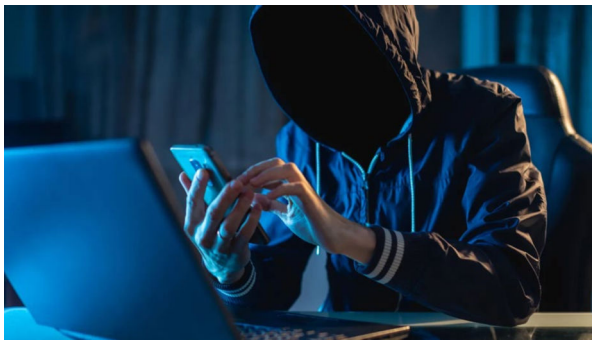

Figure 3: Vishing Attack (Source: Damiani, 2019)

b. "*IoT Vulnerabilities and Attacks: SILEX Malware Case Study*"

The Internet of Things (IoT) connects physical items to a digital environment, with 64 billion devices expected to be connected by 2025. However, this rapid growth has led to new cyber threats, particularly in Industrial IoT (IIoT), where cybercriminals exploit weaknesses to launch DDoS attacks. The SILEX virus, an asymmetric cyberthreat, targets IoT devices with default passwords. To mitigate IoT risks, strong authentication, frequent updates, security awareness, supply chain security, and incident response procedures are necessary. Future research will focus on lightweight SILEX malware mitigation and AI-based security solutions (Mukhtar et al., 2023).

V. STATISTICS OF FINANCIAL LOSSES TO IOT CYBERATTACKS

While the Internet of Things (IoT) has significantly advanced many industries, it has also raised cybersecurity threats and resulted in financial losses from cyberattacks, as seen in Figure 4.

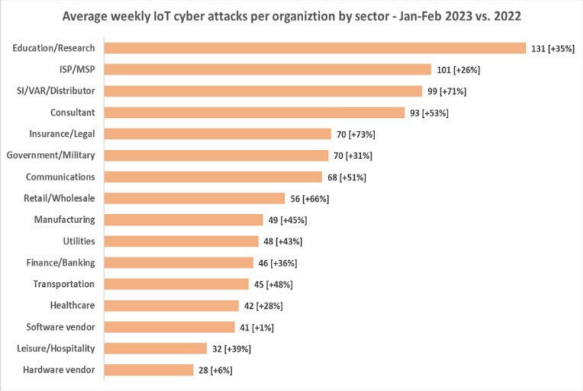

Figure 4: Statistic of IoT Cyberattacks Losses (Source: Check Point, 2023)

IoT hacks have a shocking financial effect, according to recent statistics (Hacker, 2019). Global financial damages from IoT-related cyber-attacks reached over $11.8 billion in 2020 alone. This figure illustrates the expanding risk surrounding IoT devices and shows a significant rise from previous years (Özdemir & Hekim, 2018).

The extensive use of connected devices in many businesses is one of the main causes of the significant financial losses linked to IoT hacks. The growth of IoT devices has increased the attack space for hackers, from wearables and smart homes to industrial IoT systems and smart city infrastructure. Because of this, both people and companies are susceptible to a variety of cyberthreats, such as ransomware attacks, botnet attacks, and data breaches.

IoT hacks have the potential to cause significant financial losses, especially in the healthcare industry. Healthcare organisations reported financial damages from cyber events involving medical IoT devices of an estimated $13.8 billion in 2021. These assaults not only cause financial losses but also seriously jeopardise patient safety and data privacy, underscoring the vital need for implementing strong cybersecurity safeguards in healthcare IoT installations.

Manufacturing is another area that has been severely attacked by IoT hacks. Industrial IoT (IIoT) devices are being used more and more in manufacturing facilities for automation and data analytics, making them attractive targets for hackers. Manufacturing businesses reported losses from IoT-related cyber-attacks in 2022 that exceeded $9.5 billion (Bharati & Podder, 2022). These disruptions—which highlight the need for cybersecurity resilience in industrial environments—include supply chain interruptions, manufacturing outages, and intellectual property theft.

IoT cyber risks have resulted in major financial losses for the financial services sector as well. Financial institutions suffered losses from cyberattacks that targeted Internet of Things equipment, including ATMs, payment terminals, and banking apps, in 2020, amounting to over $7.2 billion (Pomerleau & Lowery 2020). These attacks demonstrate the necessity for constant monitoring and strong security measures in financial IoT networks. They vary from credential theft and fraudulent transactions to network intrusions.

In conclusion, the data pertaining to monetary losses resulting from Internet of Things hacks presents a worrisome image of the expanding influence of cyberthreats on organisations and people around the globe. As IoT installations continue to spread across companies, preventing financial losses and protecting vital systems and data require tackling cybersecurity issues and putting proactive defence plans in place.

VI. CHALLENGES AND FUTURE DIRECTIONS

With the proliferation of internet-connected devices (IoT) and the acceleration of technological advancements (Figure 5), experts predict that the number of internet-connected devices might reach 75 billion by 2025.

This shows that the use of artificial intelligence (AI) models to address security challenges in the Internet of Things (IoT) will face challenges due to the complexity and diversity of IoT ecosystems, and the vested interest of cyber fraudsters. In the future, AI must be employed as shown in figure 6 to address

specific areas to maximise the benefits of AI in mitigating IoT security issues.

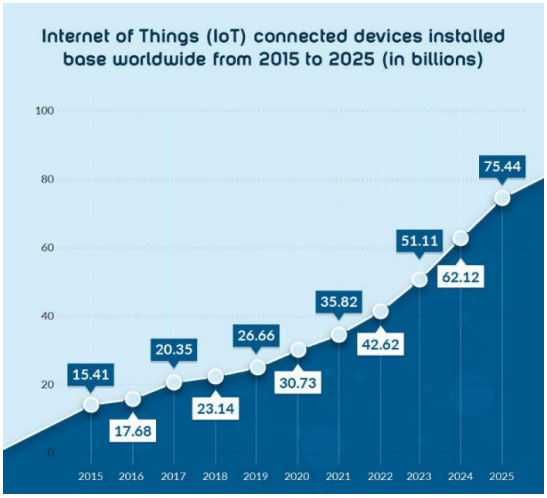

Figure 5: IoT Inter-Connected Devices by 2025 (Source: Marktechpost, 2021)

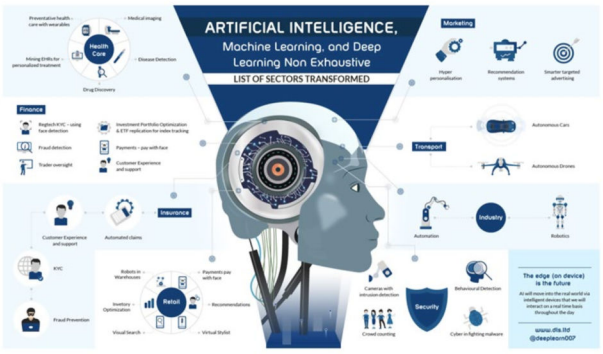

Figure 6: AI in Future of IoT (Source: Marktechpost, 2021)

Some of the areas of concern to be addressed are as follows:

1. ***Current limitations and challenges in applying AI to IoT security***: Complex IoT ecosystems, interoperable AI solutions, and standardised security frameworks are all obstacles that AI for IoT security must overcome. Challenges are encountered by real-time threat detection and AI algorithms as a result of restricted power and resource availability. AI for IoT is fostering industry collaboration on standardised security frameworks, optimising energy-efficient algorithms, and developing lightweight AI models in order to address these challenges. This could ensure a more secure future through enhanced security resilience, proactive threat detection, and dependable IoT installations.

2. ***Potential future developments and research directions:*** Scalability, interoperability, data privacy, security, and regulatory compliance are some of the obstacles that the IoT must overcome. Strong encryption to protect personal information and standardised protocols to ensure smooth communication are essential. Improvements in security may be achieved in the future by investigating new technologies such as blockchain, 6G networks, and edge computing. Algorithms for automated decision-making and predictive analytics are being created using artificial intelligence and machine learning. We are actively seeking sustainability initiatives and energy-efficient solutions to lessen the environmental effects of Internet of Things (IoT) installations.

3. ***Ethical and regulatory considerations:*** Ensuring data privacy, security, and transparency in IoT technologies while adhering to legal requirements like CCPA and GDPR is challenging. Ethical issues include addressing biases in AI systems, fair decision-making processes, and defending user rights. Future steps involve developing ethical AI frameworks, encouraging responsible data practices, and fostering cooperation between business, academia, and regulatory organizations. Improving user knowledge, permission procedures, and data security safeguards is crucial for fostering confidence in IoT technology.

VII. CONCLUSION

Artificial intelligence (AI) is being increasingly used in Internet of Things (IoT) security to improve cybersecurity by analyzing behavior, identifying

threats, and implementing automatic reactions. This technology enhances real-time vulnerability identification, mitigation, defence strengthening, and protection against evolving cyberattacks.

AI models offer advanced features like automatic reaction mechanisms, threat detection, anomaly detection, behaviour analysis, and real-time risk mitigation.

Future research should focus on AI-driven threat intelligence predictive analytics, lightweight AI models, industry-academia collaboration, and ethical and regulatory concerns related to AI security implementations.

REFERENCES

Alahi, M. E. E., Sukkuea, A., Tina, F. W., Nag, A., Kurdthongmee, W., Suwannarat, K., & Mukhopadhyay, S. C. (2023). Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends. Sensors, 23(11), 5206.

Augmented AI, (2023). The Role of Artificial Intelligence in Cybersecurity | How AI Enhances Protection. Retrieved from https://www.augmentedstartups.com/blog/the-role-of-artificial-intelligence-in-cybersecurity-how-ai-enhances-protection.

Internet of Things and artificial intelligence-driven solutions. Security and Privacy, 6(3), e285.

Alahi, M. E. E., Sukkuea, A., Tina, F. W., Nag, A., Kurdthongmee, W., Suwannarat, K., & Mukhopadhyay, S. C. (2023). Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends. Sensors, 23(11), 5206.

Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. Journal of Information Security and Applications, 82, 103748.

Bharati, S., & Podder, P. (2022). Machine and deep learning for iot security and privacy: applications, challenges, and future directions. Security and communication networks, 2022, 1-41.

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.

Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IoT: a survey. Wireless Personal Communications, 115(2), 1667-1693.

Check Point, (2023). The Tipping Point: Exploring the Surge in IoT Cyberattacks Globally. Retrieved from https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/

Damiani, J. (2019). A Voice Deepfake Was Used To Scam A CEO Out Of $243,000. Forbes. Retrieved from https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=573e64932241. 26 March, 2024

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), 4580.

Garagad, V. G., Iyer, N. C., & Wali, H. G. (2020, July). Data integrity: a security threat for internet of things and cyber-physical systems. In 2020 International Conference on Computational Performance Evaluation (ComPE) (pp. 244-249). IEEE.

Hacker, J. S. (2019). The great risk shift: The new economic insecurity and the decline of the American dream. Oxford University Press.

Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., ... & Alkhassawneh, H. M. (2022). A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. IET communications, 16(5), 421-432.

Inuwa, M. M., & Das, R. (2024). A comparative analysis of various machine learning methods for anomaly detection in cyber-attacks on IoT networks. Internet of Things, 101162.

Jurcut, A., Niculcea, T., Ranaweera, P., & Le-Khac, N. A. (2020). Security considerations for Internet of Things: A survey. SN Computer Science, 1, 1-19.

Kavitha, S., Bora, A., Naved, M., Raj, K. B., & Singh, B. R. N. (2021). An internet of things for data security in cloud using artificial intelligence. International Journal of Grid and Distributed Computing, 14(1), 1257-1275.

Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W. C. (2021). Internet of things: Evolution, concerns and security challenges. Sensors, 21(5), 1809.

Marktechpost, (2012). The Future Direction and Vision for AI. Retrieved from https://www.marktechpost.com/2021/11/05/the-future-direction-and-vision-for-ai/

Mukhtar, B. I., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). IoT vulnerabilities and attacks: SILEX malware case study. Symmetry, 15(11), 1978.

Nagaty, K. A. (2023). Iot commercial and industrial applications and AI-powered IoT. In Frontiers of Quality Electronic Design (QED) AI, IoT and Hardware Security (pp. 465-500). Cham: Springer International Publishing.

Özdemir, V., & Hekim, N. (2018). Birth of industry 5.0: Making sense of big data with artificial intelligence,"the internet of things" and next-generation technology policy. Omics: a journal of integrative biology, 22(1), 65-76.

Pomerleau, P. L., & Lowery, D. L. (2020). Countering Cyber Threats to Financial Institutions. A Private and Public Partnership Approach to Critical Infrastructure Protection. Springer.

Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: a survey. The Journal of Supercomputing, 76, 5320-5363.

Shrivastwa, R. R. (2023). Enhancements in Embedded Systems Security using Machine Learning (Doctoral dissertation, Institut Polytechnique de Paris).

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. Electronics, 9(11), 1864.

Stupp, C. (2019). Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. Retrieved from https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402. 26 March, 2024.

Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.

Torğul, B., Şağbanşua, L., & Balo, F. B. (2016). Internet of things: a survey. International Journal of Applied Mathematics Electronics and Computers, (Special Issue-1), 104-110.

Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. Ieee Access, 8, 153826-153848.

Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. Ieee Access, 9, 94668-94690.

