Artificial Intelligence and IoT security

Sai Krishna Rachamadugu

***Abstract*—** Internet of Things is shaping the quality of living standard. With the rapid growth and expansion of adopting IoT-based approaches, their security represents a growing challenge for both manufacturers and consumers. There is a recent rising trend towards employing artificial intelligence approaches to enhance the security of IoT infrastructure. This paper focuses on reviewing recent developments in applying artificial intelligence to intrusion detection in the IoT domain. Selected articles are classified according to the applied AI algorithm. This study provides an in-depth survey highlighting the recent advances in artificial intelligence for improving the security of IoT.

I. INTRODUCTION

Artificial Intelligence (AI) and the Internet of Things (IoT) have revolutionized the industrial level through efficiency and accuracy in business processes. The synergy of these technologies has played vital roles in innovative integrated solutions through authentication and computing. Since 2005, the concept of IoT proposed by the International Telecommunication Union has fostered communication and interconnection [1]. The combined sensors and devices used in the distributed network of IoT include sensors, Radio Frequency Identification Devices (RFID), Quick Response (QR) Code devices, barcodes, etc. On the other hand, AI-based countermeasure solutions have played a vital role in enhancing security performance. The modern advancements of AI in machine learning (ML) and Deep Learning (DL) have been able to detect malicious behaviour within the network [2]. AI-based security mechanisms are one of the most powerful methods for dealing with vulnerabilities. AI enables faster authentication detection and detects malicious data injection attacks in the IoT network. The application of AI benefits several industries including finance, healthcare, retail, hospitality, transportation, and many more.

This report highlights the role of AI in the IoT domain along with identifying its application areas. Significant drawbacks have also been identified where industries need to enhance its AI and IoT domain for strengthening security systems.

Role of AI in IoT devices

AI is the underlying mechanism behind IoT and hence the union of these technologies is referred to as AI-IoT [3]. The role of AI-IoT has been observed during the COVID-19 pandemic where it has measured the oxygen saturation level of blood, identified breathing difficulty, body temperature, and geo-fencing. AI-IoT has been beneficial from a technical and application perspective with its architecture, availability, and significance. Modern-day AI solutions have introduced the concept of ML and DL. A shallow ML approach is also undertaken to combat different types of attacks in the network [2]. The below diagram clarifies the role of AI technologies in dealing with serious attacks:

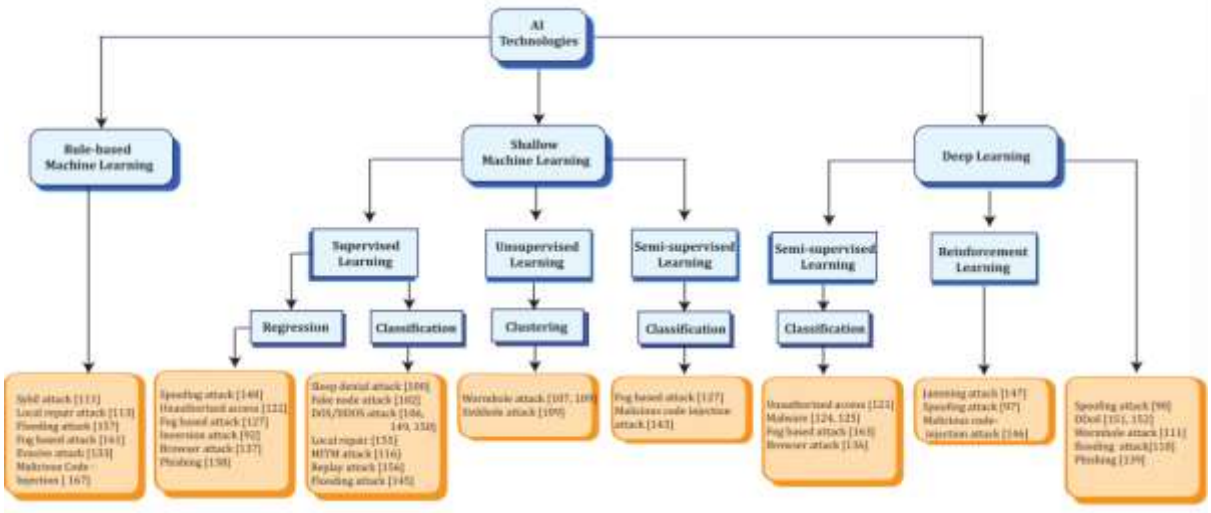

Figure 1: AI technologies dealing with attacks

(Source: [2])

The AI technologies include the implementation of complex algorithms to detect anomalous behaviour in the network. These algorithms include decision trees, linear regression, Support Vector Machine (SVM), neural networks, and several machine learning approaches [4]. In the cyber security domain, AI is considered the most common method of intrusion detection as it analyses patterns in the dataset through intelligent decision-making based on real-time data.

IoT is capable of sensing, identifying, and authenticating enabling feasible transmission and communication relying on data computing and processing technologies [1]. The architecture of IoT operates in three layers: terminal perception, network transport, and application service layer. This architecture is depicted in the below diagram:

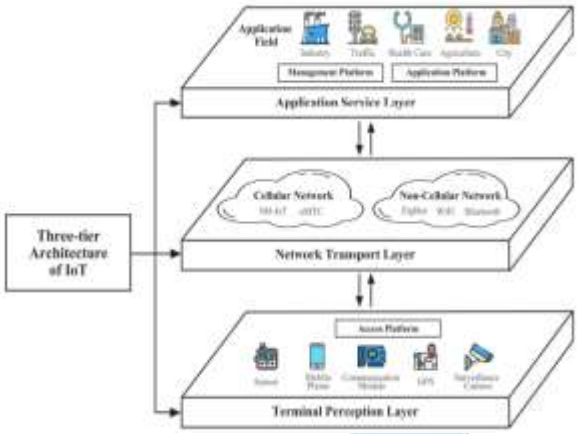

Figure 2: Architecture of IoT

(Source: [1])

AI-driven technologies are incorporated by the industrial sectors to enhance proactive mechanism processes empowering risk mitigation procedures and safeguarding sensitive information [5]. AI plays a multifaceted role in threat detection, vulnerability assessment, incident response, and predictive analysis. On the other hand, IoT enables convenience and automation. The industrial sectors implement robust encryption protocols for upgrading security in the IoT environment. The AI ecosystem gets enhanced through the incorporation of machine learning processes. AI has improvised the role of IoT leading to intelligent resource scheduling and upgrading infrastructure for profit maximisation of the devices [6]. IoT aided by AI and big data has covered a wider spectrum of applications like speech recognition, robotics and automation, etc. The popularity of AI and IoT has gone so far that it is expected that internet-connected devices will reach more than 500 billion by 2025. AI intersection and its application areas are depicted in the below diagram:

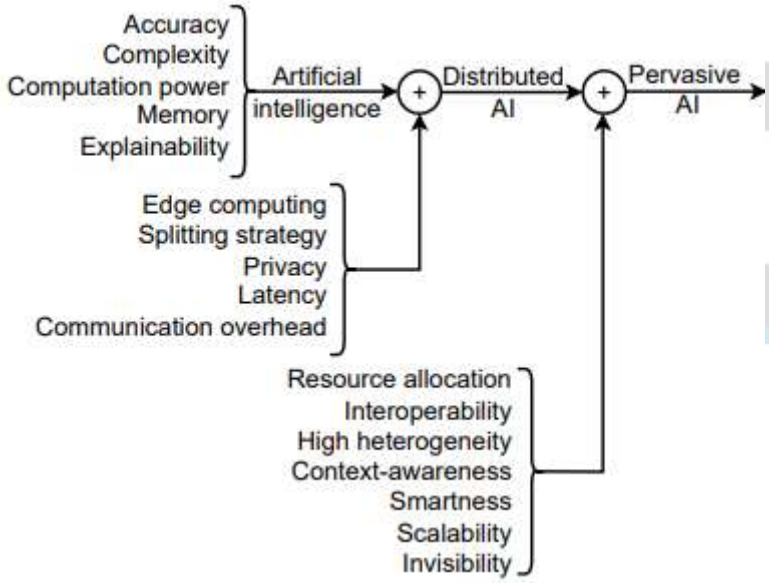

Figure 3: AI Intersection and applications

(Source: [6])

As depicted in the above diagram, the various aspects of AI-based systems include adding accuracy, dealing with complexity, and enhancing computational power. The distributed and pervasive AI ensures privacy, communication, resource allocation, interoperability, scalability, and heterogeneity in various business domains.

Industrial applications of AI and IoT security

Several industries across the world implement AI and IoT to strengthen security and optimize business procedures. These industries include healthcare, retail, finance, hospitality, transportation, and many more. In the healthcare industry, the integration of AI and IoT enables improved medical diagnosis and improved treatment capabilities. The blend of these technologies has ensured the security of patients' data by implementing privacy protection technology [7]. On the other hand, the tourism and retail industry has benefitted from AI and IoT technology. In the tourism industry, the automated guest check-in procedure, smart hotel rooms, and motorised curtains are operated by IoT-enabled door lock security systems. Customer satisfaction is also ensured through adding safety and security during hotel stays adding peace of mind for the guests [8]. In the retail sector, IoT has been implemented through RFID technology. This technology has enabled access to valuable information on sales updates and the

purchasing behaviour of customers. Supply chain risks and organisational assets are identified and analysed by RFID. IoT-based inventory systems are also implemented for monitoring stock levels and product availability. Hence, the industrial sectors are greatly benefitted from the implementation of AI and IoT-based systems.

Feasibility Analysis of AI Applications in the IoT domain

In the COVID-19 era, industries have incorporated AI-IoT along with blockchain, deep learning, fog computing, etc. for dealing with the pandemic and monitoring patients' health, reducing its spread among the masses [3]. The application areas of AI-IoT infrastructure in the COVID-19 pandemic are depicted in the below diagram:

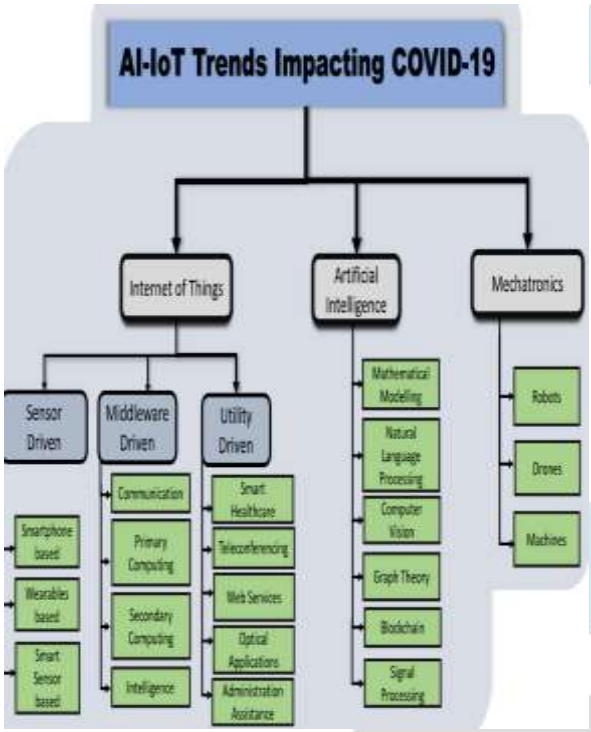

Figure 4: AI-IoT technology

(Source: [3])

Securing network and Access control: Using standardised communication protocols security and access control are ensured leading to smart business applications [9]. It enhances the real-time decision support system providing up-to-date information. Real-time visibility is highly feasible for effective decision-making and leads to organisational efficiency. Task delays are also minimised saving a lot of time. Anomalies can be also detected along with suspicious activities. The network traffic is monitored and hence unauthorised access is prevented on a wide scale.

Ensuring accuracy and robustness in intelligent sensing: The modern AI-based solutions incorporated by ML, DL, and swarm intelligence have enabled cognitive sensing using big data analytics for efficient network management [10]. AI-based IoT systems have enabled effective data processing and retrieval enhancing accuracy and robustness in intelligent sensing. Hence, various industrial sectors have incorporated this technology to obtain beneficial outcomes in business processes. The below chart shows the application domains of AI in IoT infrastructure:

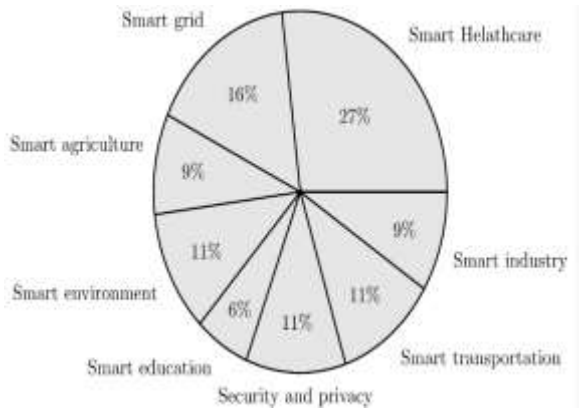

Figure 5: Statistical distribution of application domains of AI in IoT

(Source: [10])

Ensuring user authentication: AI implements several biometric authentication techniques and multi-factor authentication techniques. Unethical logic attempts are detected by examining user behaviour. As the convergence of AI and IoT is applied for adding personalization through smart assistance, it detects the voice commands and the habits and preferences of individuals [11]. This data is stored which is used for identifying vulnerable behaviour in the system. Hence, user authentication does not get compromised with the efficient implementation of this technology.

Identifying vulnerabilities: The codes designed by AI tools are analysed under the IoT domain and the files are configured accordingly. The weaknesses in the systems that can simulate attacks are identified and mitigated through security updates and patches. Hence, AI ensures significant security measures while dealing with vulnerabilities. The predictive insights identify significant risks that lead to making smarter decisions so that the risks can be prevented [11]. AI has beneficial impacts on securing the IoT infrastructure as it recognizes patterns from historical datasets to catch any threatful occurrence.

Enabling intelligent decision-making: AI-based IoT systems enhance time and cost reduction leading to flexible and streamlined business processes. AI-based decision-making facilitates efficient product scheduling [12]. The automated decision-making system lowers industrial risks by ensuring security and privacy. For intelligent decision-making, a random forest algorithm is often preferred. Organisations gain efficiency through upgrading their operational performance. Hence, industries gain a competitive advantage with the implementation of AI-IoT systems.

Drawbacks

Cyber attackers often find ways to exploit AI to perform several types of attacks [4]. Attackers often implement malicious AI to attack IoT systems. These attacks include data poisoning and input attacks. On the other hand, the resilient security framework of AI in IoT can help in withstanding the challenges and providing a comprehensive solution [13].

Security issues: IoT faces several security issues due to the lack of human supervision in the complex and changeable environment. The adoption of technology has led to the limitation of human resources leading to unattended terminals open for hackers [1]. On the other hand, the limited computing capacity of the IoT devices and the lack of computational resources are incapable of undertaking fine-grained security measures. Hence, the complex issues cannot be solved due to a lack of supervision, management, and resources.

Need for substantial data: AI-based algorithms require massive amounts of data for training and optimising the models. Ten times more data is required for training the models. The massive dataset might result in a serious privacy and security vulnerability [6]. Hence, industries need to undertake sophisticated defence mechanisms for the training, execution, and distribution of data. This provides a robust architecture to mitigate the challenges regarding this issue.

Incorrect threat detection due to inaccurate false-positive and false-negative outcomes: During the threat protection solution, the intrusion detection system (IDS) might come across errors that are referred to as false positives and false negatives. During the false positive state, a false alarm is generated when an acceptable behaviour is considered as an attack. But in the case of false negatives, unacceptable behaviour is often considered normal activity. These kinds of errors are serious security threats to the system. Through data augmentation and upgrading the learning process of the model, this threat can be mitigated.

High adoption costs: With the increased number of devices, the communication cost, bandwidth, and latency become quite unaffordable for many industries. Hence, they cannot implement the real-time applications and significant benefits offered by AI-IoT solutions [10]. However, in the agriculture industry, IoT has reduced cost and waste generation improving crop quality and the overall production process.

Privacy, scalability, and interoperability issues: As mentioned earlier, a substantial amount of data is required for the effective deployment of AI and IoT-based systems. With the rising volume of datasets, ensuring security, privacy, and effective scalability become quite difficult [9]. In this context, seamless communication and data exchange might get interrupted in case of large-scale industrial applications of this technology. However, these challenges can be mitigated through efficient stakeholder communication and maintaining industry standards.

Conclusion

The integration of AI in the IoT domain has significantly enhanced technological capabilities and resulted in potential benefits. It has enhanced threat detection, access control, and improved security and privacy architecture. The implementation comes across several drawbacks like incorrect threat detection, privacy, scalability, and interoperability issues, along with other security barriers. These can be mitigated through undertaking proactive measures while implementing AI and IoT technology ensuring strengthened communication and interaction in the network.

References

[1] H. Wu, H. Han, X. Wang and S. Sun, 2020. Research on artificial intelligence enhancing internet of things security: A survey. Ieee Access, 8, pp.153826-153848.

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

[3] J.I. Khan, J. Khan, F. Ali, F. Ullah, J. Bacha and S. Lee, 2022. Artificial intelligence and internet of things (AI-IoT) technologies in response to COVID-19 pandemic: A systematic review. Ieee Access, 10, pp.62613-62660.

[4] M. Kuzlu, C. Fair and O. Guler, 2021. Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of things, 1(1), p.7.

[5] N.G. Camacho, 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), pp.143-154.

[6] E. Baccour, N. Mhaisen, A.A. Abdellatif, A. Erbad, A. Mohamed, M. Hamdi and M. Guizani, 2022. Pervasive AI for IoT applications: A survey on resource-efficient distributed artificial intelligence. IEEE Communications Surveys & Tutorials, 24(4), pp.2366-2418.

[7] Z.X. Lu, P. Qian, D. Bi, Z.W. Ye, X. He, Y.H. Zhao, L. Su, S.L. Li and Z.L. Zhu, 2021. Application of AI and IoT in clinical medicine: summary and challenges. Current medical science, 41(6), pp.1134-1150.

[8] K.A. Nagaty, 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.

[9] N. Rane, S. Choudhary and J. Rane, 2023. Artificial Intelligence (AI) and Internet of Things (IoT)-based sensors for monitoring and controlling in architecture, engineering, and construction: applications, challenges, and opportunities. Available at SSRN 4642197.

[10] A. Bourechak, O. Zedadra, M.N. Kouahla, A. Guerrieri, H. Seridi and G. Fortino, 2023. At the confluence of artificial intelligence and edge computing in iot-based applications: A review and new perspectives. Sensors, 23(3), p.1639.

[11] Application of AI in IOT: Transforming Data Analysis (2024) Eyer. Available at: https://eyer.ai/blog/application-of-ai-in-iot-transforming-data-analysis/ (Accessed: 28 August 2024).

[12] H. Rasheed, 2024. Consideration of Cloud-Web-Concepts for Standardization and Interoperability: A Comprehensive Review for Sustainable Enterprise Systems, AI, and IoT Integration. Journal of Information Technology and Informatics, 3(2).

[13] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid and M. Assiri, 2024. Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey. IEEE Access.