EDUZONE: International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ), ISSN: 2319-5045
Volume 11, Issue 2, July-December, 2022, Available online at: www.eduzonejournal.com

Securing IoT using AI

Bhargavi Upadhyay

JNIY Institute, India

ABSTRACT

AI-driven security systems for IoT networks utilize advanced artificial intelligence (AI) technologies to monitor and manage connected devices in order to mitigate malicious activities which can disrupt network operations. Anomaly detection methods are used to identify traffic patterns or behaviors which show signs of suspicious activities, while learning adaptation allows the system to adjust parameters according to the threats faced. In addition, self-learning algorithms are employed to recognize patterns of IoT traffic and isolate any malicious activities which could lead to possible attacks. By leveraging machine learning capabilities, AI-driven security systems improve the security of connected devices, enabling them to respond quickly to threats and minimize any possible damage. In summary, AI-driven security for IoT systems is used to enhance the resilience of connected devices against cyber threats and protect them from malicious attacks more efficiently than traditional methods.

Keywords: IoT, AI, Cyber Threats, Protection Schemes, Connected Devices.

INTRODUCTION

AI-driven security for IoT systems refers to the utilization of artificial intelligence technologies to monitor and manage networked devices for the purpose of preventing malicious attacks [1]. This type of security is designed to improve the resilience of connected devices to cyber threats, and is especially advantageous for reducing the risk of distributed denial-of-service (DDoS) attacks.

AI systems are able to detect the attacks more effectively and quickly than traditional methods, as they have the power to continuously learn from the data collected from the environment and detect even the most subtle of changes [2]. The key elements of an AI-driven security system for an IoT system are anomaly detection, learning adaptation and self-learning algorithms.

Anomaly detection uses statistical models or machine learning techniques to monitor traffic patterns or behavior of devices to detect any unusual or suspicious activity [3]. For example, a system can detect patterns in the amount or types of traffic that are not expected or authorized. Once an anomaly is detected, the system can take action to block or throttle the suspect traffic [4].

Learning adaptation is the process of autoscaling a security system based on the conditions of its current environment [5]. This could involve adjusting parameters of various components in line with the volume and intensity of the threats faced. An intelligent security system can learn from incidents, enabling it to react more quickly to future attacks as it has learned from previous encounters with malicious actors [6].

Finally, self-learning algorithms are designed to recognize patterns of IoT traffic and isolate any suspicious activities that could lead to an attack. Self-learning algorithms have the ability to learn from mistakes, analyze trends, and distinguish between legitimate and malicious packets. This can be beneficial for rapidly evaluating an incoming packet, and then advancing certain actions accordingly. For example, an intelligent security system can determine whether to block, rate-limit, or permit a packet [7].

Overall, AI-driven security systems improve the security of connected devices, enabling them to respond quickly to threats and minimize any possible damage or disruption. By leveraging machine learning capabilities, these systems can detect malicious activities and protect against attacks more efficiently than traditional methods [8].

Architecture of AI based IoT System Security

The architecture of an AI-based IoT system security system typically consists of five layers: the data layer, the analytics layer, the security layer, the management layer, and the privacy component [9].

At the data layer, the system compiles and stores the IoT device data. This layer is responsible for collecting data from the various connected devices and compiling it into a single source for analysis. This data can include device location, battery status, temperature and other device-specific information [10].

The analytics layer uses machine learning algorithms to analyze the data and identify threats. Artificial intelligence and machine learning techniques are used to identify abnormal activity, potential malicious activity and vulnerabilities [11]. The security layer is responsible for preventing and responding to attacks. When abnormal activity is detected, or if suspicious patterns emerge, the security layer takes steps to mitigate threats and/or respond with appropriate action. This can include blocking incoming traffic or triggering alerts [12].

The management layer is responsible for the performance and overall health of the system. This layer is responsible for monitoring the performance of the system and taking steps to ensure that it is running efficiently [13].

Finally, the privacy component ensures the security and confidentiality of user data. This layer ensures that user data is protected through the implementation of encryption and other security measures [11,13].

Altogether, a well-designed AI-based IoT system security system should provide a comprehensive security architecture that effectively detects, prevents and responds to potential threats. This type of system will mitigate the risks associated with the use of IoT devices and ensure that data remains secure [14].

Characteristics of AI based IoT System Security

AI-based IoT system security combines traditional security methods with artificial intelligence (AI) to provide better protection, detection, and response against cyber threats. AI-based security solutions are designed to monitor and analyze data from connected devices and networks, spot patterns and anomalies in real-time, and provide targeted response to newly discovered threats [15].

The primary features of AI-based IoT system security include:

1) Intrusion detection and prevention: AI-based systems can detect known threats and provide timely alerts when suspicious behaviors are detected. AI-powered systems can also recognize anomalies in data and alert IT teams to investigate [16].

2) Automated responses: AI-based systems can automate security protocols and enforcement decisions, reducing IT staff workloads and enabling intelligent, automated responses to cyber threats [17].

3) Authentication and authorization: AI-based systems are often used to provide secure and personalized access to corporate networks and devices. AI can also be used to more effectively manage credentials and identities, providing a higher level of authorization and authentication [18].

4) Data loss prevention: AI-based systems can identify potentially malicious data exfiltration attempts and alert security teams to investigate [19].

5) Data analysis: AI-based systems can quickly analyze vast amounts of data and detect aberrations and suspicious patterns, enabling security teams to respond before a breach occurs [20].

Overall, AI-based IoT system security can provide a strong level of protection against cyber threats, and help organizations verify authorized access and usage of their networks and assets [21].

Advantages of AI based IoT System Security

Advantages of AI based IoT system security include better detection, prevention, and response against cyber threats, as well as improved authentication and authorization protocols for connected devices. AI-based system security offers improved data analysis and data loss prevention capabilities, enabling more efficient and accurate decision-making and automated enforcement of security protocols [22,23].

1) Enhanced Detection: AI-based system security can monitor and analyze data from connected devices and networks to detect known threats, anomalous activities, and suspicious patterns. By utilizing automated data analytics, AI systems can review and analyze large amounts of data in real-time and provide timely alerts when malicious activities are detected [24,25].

2) Automated Response: AI-based security systems can automate security protocols and enforcement decisions, reducing IT staff workloads and enabling intelligent, automated responses to cyber threats. AI systems can also provide more efficient and intelligent enforcement of security protocols, allowing IT staff to better focus their workloads on more strategic tasks [26].

3) Improved Authentication and Authorization: AI-based security systems can provide a more secure and personalized access to corporate networks and devices. AI-based systems can also manage credentials and identities more effectively, providing a higher level of authentication and authorization [27].

4) Data Loss Prevention: AI-based systems can identify potentially malicious data exfiltration attempts and alert security teams to investigate [28].

5) Improved Data Analysis: AI-based systems can quickly analyze vast amounts of data and detect aberrations and suspicious patterns, enabling security teams to respond before a breach occurs. This allows organizations to be proactive against cyber threats, as opposed to reactive [29].

Challenges and Open Issues in AI based IoT System Security

One of the major challenges of AI-based IoT system security is dealing with the sheer volume of data generated by connected devices. As the number of IoT devices expands, the resulting data volumes and complexity can vastly exceed current organizational capacity [30]. This leads to well-known challenges such as data blindness, where the sheer volume of data makes it difficult to detect patterns, and data latency, where real-time data arrives too late to be useful. Additionally, AI-based systems need to be trained on existing IoT data, which is often incomplete, inconsistent and noisy.

This makes AI algorithms vulnerable to bias and errors, resulting in false positive and false negative predictions, leading to security vulnerabilities [31].Another open issue regarding AI-based IoT system security is the lack of transparency. As AI algorithms become increasingly complex, humans have difficulty understanding and interpreting their predictions and outcomes. This has significant implications for ensuring the proper functioning of these systems and the security of assets, since organizations are unable to properly assess their security posture [32].Finally, organizations need to be careful about the type of data collected and shared, as data privacy will play a critical role in the success and adoption of AI-based IoT systems. Organizations must protect user data from unauthorized access, and adhere to relevant laws and regulations. In addition, companies must provide users with meaningful controls over their own data, such as the ability to delete or modify information. As AI systems are increasingly powering IoT devices and applications, organizations need to integrate robust data privacy practices to ensure user trust [33].

CONCLUSION

In conclusion, AI-based IoT system security offers numerous advantages for organizations looking to protect their infrastructure and data from malicious cyber activities. By utilizing automated analytics, enhanced detection of cyber threats, improved authentication and authorization, automated enforcement of security protocols, and improved data analysis, organizations can greatly improve their defense against malicious actors. Furthermore, AI-based systems can reduce the workload of IT staff and provide more efficient and intelligent protection against data exfiltration attempts. AI-based system security provides an overall greater degree of protection, requiring less human intervention and enabling organizations to better protect their business operations.AI-based IoT system security can provide value to organizations in multiple ways. For starters, it can analyze data faster and more accurately, while improving detection of cyber threats. Advanced analytics and machine learning can be used to uncover previously undetected threats, as well as to detect patterns of misuse. Moreover, AI-based systems can reduce the workload of IT staff by automating processes such as authentication and authorization, enforcing security protocols, and analyzing data. Finally, AI-based systems can provide an overall better experience, with less manual intervention and higher levels of security. With the current climate of cyber threats and data breaches, AI-based IoT system security offers a strong defense against malicious actors, providing organizations with the tools they need to protect their infrastructure and data.

REFERENCES

[1]. Rathore, R.S., Hewage, C., Kaiwartya, O. and Lloret, J., 2022. In-vehicle communication cyber security: challenges and solutions. *Sensors*, *22*(17), p.6679.
[2]. D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, “Next century challenges: Scalable coordination in sensor networks,” in Proc. Int. Conf. Mobile Computing and Networking (MOBICOM), 1999, pp. 263–270.
[3]. Rathore, R.S., Kaiwartya, O., Qureshi, K.N., Javed, I.T., Nagmeldin, W., Abdelmaboud, A. and Crespi, N., 2022. Towards enabling fault tolerance and reliable green communications in next-generation wireless systems. *Applied Sciences*, *12*(17), p.8870.
[4]. Khasawneh, A.M., Singh, P., Aggarwal, G., Rathore, R.S. and Kaiwartya, O., 2022. E-Mobility Advisor for Connected and Autonomous Vehicles Environments. *Adhoc& Sensor Wireless Networks*, *53*.
[5]. Kumar, S., Rathore, R.S., Mahmud, M., Kaiwartya, O. and Lloret, J., 2022. BEST—Blockchain-Enabled Secure and Trusted Public Emergency Services for Smart Cities Environment. *Sensors*, *22*(15), p.5733.
[6]. Jha, S.K., Prakash, S., Rathore, R.S., Mahmud, M., Kaiwartya, O. and Lloret, J., 2022. Quality-of-service-centric design and analysis of unmanned aerial vehicles. *Sensors*, *22*(15), p.5477.
[7]. Kumar, M., Kumar, S., Kashyap, P.K., Aggarwal, G., Rathore, R.S., Kaiwartya, O. and Lloret, J., 2022. Green communication in internet of things: A hybrid bio-inspired intelligent approach. *Sensors*, *22*(10), p.3910.

[8]. Rathore, R.S., Sangwan, S., Kaiwartya, O. and Aggarwal, G., 2021. Green communication for next-generation wireless systems: optimization strategies, challenges, solutions, and future aspects. *Wireless Communications and Mobile Computing*, *2021*, pp.1-38.
[9]. Rathore, R.S., Sangwan, S. and Kaiwartya, O., 2021. Towards Trusted Green Computing for Wireless Sensor Networks: Multi Metric Optimization Approach. *Adhoc& Sensor Wireless Networks*, *49*.
[10]. Rathore, R.S., Sangwan, S., Adhikari, K. and Kharel, R., 2020. Modified echo state network enabled dynamic duty cycle for optimal opportunistic routing in EH-WSNs. *Electronics*, *9*(1), p.98.
[11]. Rathore, R.S., Sangwan, S., Mazumdar, S., Kaiwartya, O., Adhikari, K., Kharel, R. and Song, H., 2020. W-GUN: Whale optimization for energy and delay-centric green underwater networks. *Sensors*, *20*(5), p.1377.
[12]. Rathore, R.S., Sangwan, S., Prakash, S., Adhikari, K., Kharel, R. and Cao, Y., 2020. Hybrid WGWO: whale grey wolf optimization-based novel energy-efficient clustering for EH-WSNs. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), pp.1-28.
[13]. Singh, U.P. and Rathore, R.S., 2013. Distributed Hierarchical Group Key Management using Elliptic Curve and Hash Function. *International Journal of Computer Applications*, *61*(19).
[14]. Singh, U.P. and Rathore, R.S., 2012. An efficient distributed group key management using hierarchical approach with ECDH and symmetric algorithm. *J. Comput. Eng. Intel. Syst*, *3*(7), pp.32-41.
[15]. C.Y. Chong, F. Zhao, S. Mori, and S.Kumar, "Distributed tracking in wireless ad hoc sensor networks," in Proc. 6th Int. Conf. Information Fusion, 2003, pp. 431–438.
[16]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Routing Protocol for MANETs: A Survey. *IUP Journal of Computer Sciences*, *4*(3).
[17]. Bali, V. and Rathore, R.S., 2010. A NEW HIERARCHICAL TRANSACTION MODEL FOR MOBILE ADHOC NETWORK ENVIRONMENT. *International Journal on Computer Science and Engineering*, *2*(3).
[18]. Singhal, S. and Rathore, R.S., 2015. Detailed Review of Image Based Steganographic Techniques. *IJCST*, *6*, pp.93-95.
[19]. Kumar, V. and Rathore, R.S., 2018, October. Security issues with virtualization in cloud computing. In *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* (pp. 487-491). IEEE.
[20]. Sharma, P. and Rathore, R.S., 2015. Three Level Cloud Computing Security Model. *International Journal of Computer Applications*, *119*(2).
[21]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, August. Information Technology Architectures for Grid Computing and Applications. In *2009 Fourth International Multi-Conference on Computing in the Global Information Technology* (pp. 52-56). IEEE.
[22]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Performance analysis of priority scheme in ATM network. *International Journal of Computer Applications*, *1*(13), pp.26-31.
[23]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, December. A Framework to Provide a Bidirectional Abstraction of the Asymmetric Network to Routing Protocols. In *2009 Second International Conference on Emerging Trends in Engineering & Technology* (pp. 1143-1150). IEEE.
[24]. Dixit, R., Gupta, S., Rathore, R.S. and Gupta, S., 2015. A novel approach to priority based focused crawler. *International Journal of Computer Applications*, *116*(19).
[25]. Tomar, R. and Rathore, R.S., 2016. Privacy Preserving in TPA using Secured Encryption Technique for Secure Cloud. *International Journal of Computer Applications*, *138*(8).
[26]. Tomar, R. and Rathore, R.S., 2016. A Survey on Privacy Preserving in TPA Using Secured Encryption Technique for Secure Cloud. *International Advanced Research Journal in Science, Engineering and Technology*, *3*(4), pp.83-86.
[27]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Clustering Technique Approach to Detect the Special Patterns for Medical Video Mining. *Advances in Data Management*, p.140.
[28]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Architectural Options and Challenges for Broadband Satellite ATM networks. *Recent Developments in Computing and Its Applications*, p.155.
[29]. Srivastava, S.N., Kshatriya, S. and Rathore, R.S., 2017. Search Engine Optimization in E-Commerce Sites. *International Research Journal of Engineering and Technology (IRJET)*, *4*(5), pp.153-155.
[30]. Rattan, V., Sinha, E.M., Bali, V. and Rathore, R.S., 2010. E-Commerce Security using PKI approach. *International Journal on Computer Science and Engineering*, *2*(5), pp.1439-1444.
[31]. Bali, V., Rathore, R.S. and Sirohi, A.,2010. Adaptive Analysis of Throughput in Mobile Admhoc Network (IEEEm802. 11).*International Journal of Computer Science & Communication*, *1*(1), pp.25-28.
[32]. Kumar, V. and Singh Rathore, R., 2016. A Review on Natural Language Processing. *International Journal Of Engineering Development And Research*.
[33]. Bhatnagar, D. and Rathore, R.S.,2015. CLOUD COMPUTING: SECURITY ISSUES AND SECURITY MEASURES. *International Journal of Advance Research in Science And Engineering*, *4*(01), pp.683-690.