EDUZONE: International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ), ISSN: 2319-5045
Volume 12, Issue 1, January-June, 2023, Available online at: www.eduzonejournal.com

Intelligent Internet of Things

Vaibhav Sharan

Ishan Institute, India

ABSTRACT

Recent advances in networking has brought about a substantial transformation in the handling and transport of data.This was made possible by the tremendous advances in wireless communication technology and the development of distributed computing and machine learning technologies. These advancements enable much faster processing of data and the ability to quickly and accurately detect anomalies in the data. As a result, this has enabled the creation of connected systems and services that operate on the move or in an environment with varying conditions, such as the Internet-of-Things (IoT), Internet-of-Vehicles (IoV), and the Internet-of-Drones (IoD). It is a security tool which is designed to monitor activity on a network and identify potentially malicious activity. It typically features a combination of signature-based detection, which looks for activity that matches a known pattern of malicious activity, and anomaly-based detection, which involves the use of artificial intelligence techniques to detect unusual behaviour. An IDS system also usually includes active response capabilities which can take action on malicious activity as soon as it is detected, such as blocking the source or quarantining the malicious code. This research is based upon, the application of Intrusion Detection Systems (IDS) in SDN-based IoT networks, which is important for ensuring security of these networks. SDN provides an enhanced level of control over the entire system, making it an attractive target for cyber criminals. An IDS can be used to detect malicious activity such as port scans, DDoS attacks, and other types of malicious traffic. An IDS can also help to detect unauthorized access to the control plane of the network, which is a potential way for attackers to gain control of the IoT devices. Additionally, IDS systems can be used to protect against malware and other malicious activities, as well as provide detailed forensic reports of malicious activity. The use of an IDS in SDN-based IoT networks can help protect these systems from intrusion and malicious activity, and ensure the security of these valuable IoT networks.

Keywords: IOT, IDS (Intrusion Detection Systems), Computer networks, IoV, IoD

INTRODUCTION

Flexibility of connection and highly-effective security tools are essential for IOT networks because they enable the network to adapt to different types of devices, new protocols, and increased data loads. Furthermore, they protect the network against malicious attacks and unauthorised access [1]. By using encryption, authentication, and authorization protocols, organizations can ensure that the data within their IOT network remains secure [2]. Additionally, by deploying Virtual Private Network (VPN) connections, individuals or organizations can further protect their data from potential eavesdroppers and malicious actors [3].

It is a concept that involves connecting devices to the internet in order to send and receive data [4]. This is enabled through the use of numerous advanced technologies such as Wi-Fi, NFC, Bluetooth, 5G, and other wireless networks. As this technology advances, it will enable objects to become connected to the internet from anywhere, no matter how remote, transforming access to data and communication with unprecedented levels of convenience [5]. This will drastically reduce the time and energy it takes to coordinate physical infrastructure and achieve joint goals, while also introducing a plethora of easy-to-use applications that make complex tasks easier to pursue [6]. Ultimately, the increasing interconnectedness of IoT will provide individuals, businesses, and governments with more opportunities to become more efficient, efficient and productive [7].

For example, a successful attack on an IOT device could be used to gain access to other devices within the network or even the underlying physical infrastructure [8]. In order to protect against this type of attack, organizations must also deploy advanced intrusion detection and response tools and strategies, as well as robust access control strategies [9].

In summary, flexibility and security of IOT networks are essential to protect against malicious attacks, ensure data privacy, and enable the network to adapt to changing demands [10]. Organizations must remain vigilant and deploy advanced security tools, such as authentication protocols, encryption, and VPN connections, to protect the data within their IOT networks. Additionally, they must adopt robust access control and intrusion detection and response strategies to mitigate any potential vulnerabilities [11].

The fifth-generation of wireless technology (5G) marks a substantial leap in capability and performance compared to earlier versions. Its ultra-low latency, high data speeds, and reliability make it the ideal foundation for creating a new and better connected world. 5G allows for improved scalability, reliability, and security for infrastructure, providing a foundation for the highly interconnected world of the Internet of Things (IoT) [12] . Advanced 5G networks will be essential for the implementation of smart cities, connected vehicles, connected homes, and more. Many of these technologies require stable, high-speed connectivity in order to provide the best user experience, and 5G is one of the most capable technologies for this purpose [13]. 5G networks are also enabling more powerful edge computing, which can help reduce latency and enable data to be processed more quickly [14]. This makes 5G essential for the future of IoT and its development—and, consequently, of our lives as they become more digitally connected [15].This paper discusses how Finite State Machines (FSMs) can be used to identify and detect threats from malicious attacks on the IoT networks [16]. We propose a novel FSM based anomaly detection system which uses a combination of probabilistic, rule based and supervised machine learning techniques to identify malicious activities [17]. We analyze the results of our experiment with various FSM models to assess the performance of our system. We then propose some additional measures which may further improve the performance of our anomaly detection system. Finally, we conclude our article by providing some future directions for research in this area [18].

Overall, the use of automata and FSM based anomaly detection systems can provide a more secure and improved security mechanism for customers using IoT devices [19]. Through the use of authentication, authorization, encryption and other security measures, intrusions and malware can be prevented to ensure the safety of user data. Furthermore, the use of FSM models provides an effective and efficient way to detect malicious activities on the networks and aid in providing increased security for IoT users [20].

Background of The Research

The popularity and widespread utilization of Internet of Things (IoT) devices have opened up a vast array of security concerns. IoT networks are highly vulnerable to malicious attacks and can result in catastrophic damages if not properly secured [21]. Malicious attacks can compromise confidential information and compromise user security. In order to ensure that these devices are kept out of malicious reach, it is important to employ advanced security mechanisms to protect them from potential threats [22].

One promising security measure is the use of finite state machines. Finite state machines (FSMs) provide an efficient technique for recognizing and representing complex events. They also enable decentralized security management as they are easily scalable in size [23]. Furthermore, they provide a rigorous framework for specifying and enforcing rules and regulations which are essential for detecting malicious activity on the networks [24]. The application of FSMs in anomaly detection can help in identifying malicious activities on the networks and alert the users before the malicious attack is inflicted [25].

In this paper, we will explore the effectiveness of FSMs in detecting malicious activities on the networks. Specifically, we will utilize the principles of probabilistic machine learning, rule-based learning, and supervised machine learning to build an initial anomalous event detection system [26]. We will also utilize an online machine learning system based on FSMs to test the effectiveness of our proposed anomaly detection system. We will then present additional measures for further improving the performance of our system. Finally, we will discuss the future direction for research in this area [27].

Intrusion Detection System

The concept of intrusion detection has been around for centuries. For example, in 19th century France, guard dogs were used to detect intruders in castles. Since then, the development of advanced technologies has allowed for the automation of detection systems [28]. In the 1950s, the first electronic intrusion detection system was developed by Clarence "Jerry" Darling, a physicist working at MIT. The system worked by using vibration sensors to detect changes in temperature, sound, and other physical indicators of potential intruders [29].

In the 1960s and 70s, intrusion detection systems began to include sophisticated computer algorithms to analyze data such as intruder-generated commands, which could be used to identify malicious activities [30]. The US military also developed and applied rule-based approaches to detect anomalies in network traffic [31].

However, it was not until the 1990s that intrusion detection technology began to be widely used and accepted by the public [32]. This was due in part to the increasing sophistication of attack techniques, as well as the development of intelligent intrusion detection systems (IDS) [33]. In 1998, the US government produced their "Intrusion Detection System Strategic Plan" which served as the first formal platform for utilizing intrusion detection systems [34]. Since then, the use of IDS has become more widespread and sophisticated, allowing for a more effective defence against malicious activities [35].

Types of Intrusion detection systems

1. Network-based intrusion detection systems (NIDS)

It monitors traffic on a network. They look for suspect traffic, verify that it is malicious, and then trigger alarms to alert system administrators about the threat [36]. NIDS are often placed at key entry points in a network, such as firewalls, to monitor incoming and outgoing traffic [37]. They use sophisticated analysis and monitoring methods to detect anomalous traffic patterns, unknown protocolsand denial of service attacks [38].

2. Host-based Intrusion Detection Systems (HIDS)

These are the software programs that monitor system and application logs to detect malicious activities from within the network. HIDS are installed on individual systems within a network, such as servers, and examine the activities of system processes and users. They use signature-based detection (i.e. known attacks) and anomaly-based detection (i.e. unknown attacks) to identify malicious activities, such as unauthorized user access, privilege escalations, and malware executions [39].

3. Common datasets used in intrusion detection systems (IDS)

It includes NIST National Vulnerability Database (NVD), which is a repository of publicly known information security vulnerabilities, and other sources of malicious activity such as log events, system snapshots, and network traffic [40]. Datasets can be used to generate metrics and models that are used to detect suspicious activities [41].Additionally, datasets can be used to train machine learning algorithms and create anomaly-based models that can detect novel threats [42].

CONCLUSION

These applications offer a wide range of benefits, such as energy and cost savings, improved user experience, and enhanced security. To ensure the security of these applications, though, it is important to implement intrusion detection systems (IDS) that can detect and respond to malicious traffic and unwanted behaviour. IDS systems can be used to monitor traffic patterns and detect malicious activities such as unauthorized access, port scans, and data leakage in real time. In the wrong hands, sensitive data can be stolen or manipulated, leading to security breaches and financial losses. To protect IoT devices, it is important to implement intrusion detection systems (IDS) that can monitor and detect anomalies in network traffic and alert users of potential threats. Additionally, IDS can be used to detect malicious activities such as unauthorized access, port scans, and data leakage in real time, providing an extra layer of security for IoT devices.

REFERENCES

[1]. 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*.

[2]. Rathore, B., 2023. Textile Industry 4.0: A Review of Sustainability in Manufacturing. *International Journal of New Media Studies (IJNMS)*, *10*(1), 38–43.

[3]. Fabijan A. Corneal endothelium image segmentation using feedforward neural network: Proceedings of the Federated Conference onComputer Science and Information Systems; IEEE Cataloge Number, 2017:629-637.

[4]. Rathore, B., 2023. Future of Textile: Sustainable Manufacturing & Prediction via ChatGPT. *International Journal of New Media Studies (IJNMS)*, *10*(2), 58–69.

[5]. 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.

[6]. 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.

[7]. Rathore, B., 2021. Fashion Transformation 4.0: Beyond Digitalization & Marketing in Fashion Industry. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *10*(2), pp.54-59.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. Rathore, B., 2022. Textile Industry 4.0 Transformation for Sustainable Development: Prediction in Manufacturing & Proposed Hybrid Sustainable Practices. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *11*(1), pp.223-241.

[12]. Rathore, R.S., Hewage, C., Kaiwartya, O. and Lloret, J., 2022. In-vehicle communication cyber security: challenges and solutions. *Sensors*, *22*(17), p.6679.
[13]. 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*.
[14]. 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.
[15]. 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.
[16]. 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.
[17]. 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.
[18]. 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.
[19]. 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).
[20]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Routing Protocol for MANETs: A Survey. *IUP Journal of Computer Sciences*, *4*(3).
[21]. 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).
[22]. Singhal, S. and Rathore, R.S., 2015. Detailed Review of Image Based Steganographic Techniques. *IJCST*, *6*, pp.93-95.
[23]. 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.
[24]. Sharma, P. and Rathore, R.S., 2015. Three Level Cloud Computing Security Model. *International Journal of Computer Applications*, *119*(2).
[25]. 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.
[26]. 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.
[27]. 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.
[28]. Rathore, B., 2022. Impact of Green Marketing on Sustainable Business Development. Cardiff Metropolitan University. Presentation.
[29]. 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).
[30]. 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).
[31]. 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.
[32]. 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.
[33]. 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.
[34]. Rathore, B., 2023. Digital Transformation 4.0: A Case Study of LK Bennett from Marketing Perspectives. *Eduzone: International Peer Reviewed/Refereed MultidisciplinaryJournal*, *12*(1), pp.40-49.
[35]. Bhusan, M., Rathore, R.S. and Jamshed, A., 2018. *Fundamental of Cyber Security: Principles, Theory and Practices*. BPB Publications.
[36]. 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.
[37]. Rathore, B., 2023. Integration of Artificial Intelligence & It's Practices in Apparel Industry. *International Journal of New Media Studies (IJNMS)*, *10*(1), pp.25-37.
[38]. Bali, V., Rathore, R.S. and Sirohi, A., Adaptive Analysis of Throughput in Mobile Admhoc Network (IEEEm802. 11).
[39]. Saxena, S., Rathore, R.S., 2013. *Compiler Design*. S. Chand Publishing.

[40]. Kumar, V. and Singh Rathore, R., 2016. A Review on Natural Language Processing. *International Journal Of Engineering Development And Research*.
[41]. Rathore, B., 2022. Supply Chain 4.0: Sustainable Operations in Fashion Industry. *International Journal of New Media Studies (IJNMS)*, *9*(2), pp.8-13.
[42]. Rathore, B., 2023. Digital Transformation 4.0: Integration of Artificial Intelligence & Metaverse in Marketing. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *12*(1), pp.42-48.