Shivani Meena, 2024, 12:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

A Survey on Techniques of IOT Intrusion Detection and Feature Optimization

Shivani Meena[1], Professor Rani Kushwaha[2], Professor Jayshree Boaddh[3]

M.tect Student, Mittal Institute of technology, Bhopal[1]
Ap, CSE Mittal Institute of technology, Bhopal[2]
HOD, CSE, Vaishnavi Institute of technology and Science, Bhopal[3]

Abstract- Internet of Things (IOT) brings flexibility and control in unfavorable conditions. IOT is adapted by various businesses to provide solutions for communication. But flexibility in computer networks increases the chance of attack. Hence security of data is highly desirable to build trust in the nodes, as many solutions collect data for research, monitoring purposes. This paper summarize sophisticated techniques, including machine learning, to detect potential threats at an early stage in the IOT network. The effectiveness of IDS is closely depends on input data so optimization of the features used for detecting intrusions. Techniques such as Principal Component Analysis (PCA), Genetic Algorithms (GA), and various dimensionality reduction methods are essential for improving detection accuracy while reducing computational demands. This paper has summarize various work done by the researcher to increase the network attack detection strength of the IOT.

Keywords- Deep Learning, Intrusion Detection, Feature Optimization, Genetic Algorithm, Soft Computing.

I. INTRODUCTION

The Internet of Things (IoT) has become widely popular for its extensive potential in various sectors, such as healthcare, transportation, and smart cities. It involves connecting numerous physical devices, known as "things," within a network. These devices typically have limited computational power and storage capabilities. As the number of diverse devices increases in the IoT, a significant amount of data is generated, making IoT networks attractive targets for potential attackers.

The main challenges in IoT revolve around devices with constrained resources, low computational and storage capacities, and cybersecurity concerns [1]. Implementing essential security measures becomes challenging. In the current landscape, Machine Learning (ML) and Deep Learning (DL) techniques have emerged as suitable approaches for processing large amounts of data, leading to improved computational results. Various ML techniques are used to select optimal features from datasets, while DL methods automatically extract the best features during their application to a dataset [2].

Addressing cybersecurity in IoT networks has become a paramount concern, requiring the planning and implementation of effective Intrusion Detection Systems (IDS) at edge nodes. Over recent decades, both ML and DL-based IDSs have proven effective in detecting attacks within IoT networks. Thus, these approaches are gaining popularity in the cybersecurity realm, proving well-suited for identifying threats in IoT environments.

Nodes within an IoT network typically have limited capacity, constrained resources, and minimal manual control compared to traditional networks. These seemingly unassuming technological components often expose themselves to potential attacks, escalating concerns about their security due to the continuous emergence of new cyber threats. Various security mechanisms have been developed over the years, some effective against specific types of attacks [4]. Given the substantial data volume generated by the IoT, there is a need for efficient methodologies to detect attacks rapidly. Common forms of assaults on IoT communication channels include botnets, denial-of-service (DoS) attacks, man-in-the-middle attacks, infiltration, identity theft, data theft, ransomware, and more. Among these, botnet threats are particularly prevalent and challenging to completely thwart due to their evolving nature over time.

In [7], an enhancement in the Software-Defined Networking (SDN)-based intrusion detection and prevention system for IoT is presented. This mechanism utilizes SDN capabilities to create a proactive system designed for intrusion detection within IoT networks. The SDN-based system facilitates network programming by separating the control and data planes, providing a comprehensive global view of the network. With its programmability feature and holistic network perspective, SDN emerges as a superior alternative to address challenges encountered in ensuring the seamless operation of IoT [8,9].

II. TYPES OF IOT INTRUSION DETECTION SYSTEMS

Intrusion Detection Systems (IDS) play a vital role in maintaining the security of computer systems and networks by continuously monitoring and analyzing activity to identify any signs of malicious behavior or policy violations. IDS can be classified into five distinct categories, each serving a unique purpose and employing specific detection techniques. These categories include Misuse Detection, Anomaly Detection, Host-Based IDS, Network-Based IDS, and Hybrid IDS, as illustrated in Figure 1. Each of these types offers a different approach to intrusion detection, targeting various aspects of system and network security.

Misuse Detection focuses on identifying known patterns of malicious activity by comparing monitored activities against a database of known attack signatures. Anomaly Detection, on the other hand, aims to detect unusual behavior that deviates from established norms, making it particularly effective at identifying new or unknown threats. Host-Based IDS operates directly on individual computers or devices, monitoring and analyzing events such as file modifications, system calls, and user activities. In contrast, Network-Based IDS monitors network traffic to identify suspicious activities, such as unusual data flows or unauthorized access attempts, across the entire network. Lastly, Hybrid IDS combines elements of both Host-Based and Network-Based systems, leveraging the strengths of each to provide comprehensive protection.

The detailed elaboration for each type of IDS will be provided in the following sections, where the specific mechanisms, advantages, and challenges associated with each approach will be thoroughly explored [17].

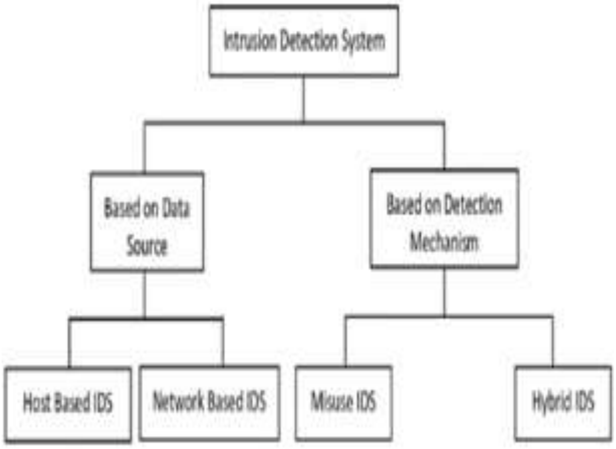

Fig. 1. Intrusion detection in IOT Networks

IDSs can be categorized based on their data sources into Host-Based IDS (HIDS) and Network-Based IDS (NIDS) [18].

Host-Based IDS (HIDS) focuses on monitoring individual computers or devices within a network by analyzing data such as system logs, application logs, and file integrity checks. HIDS is particularly useful for detecting unauthorized changes to system files or suspicious user activities on a specific host. For instance, it can identify attempts to gain unauthorized access or escalate privileges on a device.

Network-Based IDS (NIDS) monitors data as it flows across the network, capturing and analyzing packets in real-time. This type of IDS is well-suited for detecting network-level attacks like Denial-of-Service (DoS) attacks or unauthorized access attempts by identifying abnormal traffic patterns that deviate from normal network behavior.

To detect intrusions, IDSs use two primary mechanisms: anomaly-based detection and signature-based detection (misuse detection) [19]. Anomaly-based detection works by comparing current activities against a baseline of normal behavior, which is established using historical data or predefined models. This approach is effective at detecting new or previously unknown threats, as it flags any deviation from the expected behavior as a potential intrusion. However, the downside is that it may generate a high number of false positives, as legitimate but unusual activities could be misinterpreted as threats.

Signature-based detection relies on a database of known attack patterns or signatures. It monitors system or network activities for matches with these known signatures, making it highly effective at quickly and accurately identifying known threats. The limitation, however, is that it cannot detect new, unknown attacks (zero-day threats) that do not match any existing signatures.

In summary, an IDS functions by monitoring either host-level or network-level data and applies either anomaly-based or signature-based detection techniques to identify potential security breaches. The choice of data source and detection mechanism depends on the specific security needs and environment of the system being protected.

III. RELATED WORK

In their study [8], Xiu Kan and team introduced a smart way to catch bad things happening in the Internet of Things (IoT). They used a mix of smart algorithms called Adaptive Particle Swarm Optimization Convolutional Neural Network (APSO-CNN). It's like having a bunch of tiny particles working together to adjust the settings of a special computer program that looks out for problems. They made sure this program learns well by checking how good it is using a set of data.

In another research [9], Fatani and team created a security system using a mix of deep learning (like how our brains learn) and optimization methods. They first built a way to understand important features using something called CNNs. Then, they used a special method called Growth Optimizer (GO) to pick the most useful features. To make the search for these features even better, they used something called Whale Optimization Algorithm (WOA). They tested this system on different datasets to see how well it could find and stop bad things.

Saied and others [10] did a big study to see which computer learning methods work best for catching problems in IoT networks. They tried out many different methods, like Adaptive Boosting, Gradient Descent Boosting, and others. They wanted to find the one that's most accurate and fast at stopping issues in IoT networks.

Zambare and team [11] developed a technique using a special computer program called Graph Neural Network (GNN) to spot problems in virtual networks. They tested it with data from car-hacking situations, like attacks that make a car's computer act weird. The GNN program looks at patterns and figures out what kind of attack is happening.

Kalyanam and others [12] came up with a smart way to make sure the security program on IoT devices works well without using too much computer power. They used a technique called threshold-based pruning, which is like trimming unnecessary things from a big tree. They tested this method on a common computer program called LeNet, using different datasets to check if it still works well after trimming.

In their research [13], T.-T.-H. Le and team introduced a new approach to explain why the security program thinks something is wrong. They used a mix of different methods to make sure the program not only catches problems but also tells us why it thinks there's a problem. They tested this approach using special datasets that simulate real-world situations with IoT devices.

K. A. Awan and team [14] tackled the challenge of finding and stopping bad things in IoT by using a special learning method called federated learning. This is like a group of friends working together to learn and share knowledge. They trained each IoT device to recognize and predict abnormal behavior using a trust dataset with information from knowledge, experience, and reputation. This method makes it easier for the devices to work together without using too much computer power.

IV. FEATURE OPTIMIZATION

Dimensionality reduction methods are techniques used to reduce the number of input variables (features) in a dataset while retaining as much relevant information as possible. These methods are particularly valuable in Intrusion Detection Systems (IDS) to simplify models, reduce computational costs, and improve detection accuracy by eliminating redundant or irrelevant features [20, 21]. Here are some common dimensionality reduction methods:

1. Principal Component Analysis (PCA)

PCA works by finding the directions (principal components) along which the variance of the data is maximized. These components are linear combinations of the original features, ordered by the amount of variance they explain. By selecting only the top components, PCA reduces the dimensionality of the dataset while retaining the most critical information for analysis.

2. Linear Discriminant Analysis (LDA)

LDA is a supervised technique that projects the data onto a lower-dimensional space where the classes are most separable. It does this by maximizing the ratio of the between-class variance to the within-class variance. LDA is particularly effective when dealing with labeled data and is often used for feature reduction in classification tasks, including in IDS.

3. t-Distributed Stochastic Neighbor Embedding (t-SNE)

t-SNE is a non-linear technique that maps high-dimensional data to a lower-dimensional space (typically 2D or 3D) in a way that similar data points remain close together. Although primarily used for visualization, t-SNE can also help in understanding the structure of the data and selecting features that contribute to clusters of similar instances, which can be valuable in IDS for identifying patterns of attacks.

4. Autoencoders

Autoencoders are a type of neural network used for unsupervised learning. They consist of an encoder that compresses the input into a lower-dimensional representation and a decoder that reconstructs the original data from this compressed form. The middle layer (bottleneck) of the network represents the reduced-dimensional data. Autoencoders can be used to automatically extract the most significant features, reducing the dimensionality while maintaining the ability to detect anomalies.

5. Genetic Algorithms (GA)

Genetic Algorithms are inspired by the process of natural selection. They start with a population of possible feature subsets and evolve this population over several generations. In each generation, subsets are evaluated using a fitness function (e.g., the accuracy of a classifier), and the best-performing subsets are selected to create a new generation through operations like crossover (combining subsets) and mutation (randomly altering subsets). GA is particularly useful in searching large and complex feature spaces for the optimal subset of features that maximize IDS performance.

V. CONCLUSION

To summarize, the rapid growth of Internet of Things (IoT) technologies brings with it both tremendous potential and significant cybersecurity challenges. As IoT systems become more embedded in diverse industries, the likelihood of security breaches and data privacy issues increases. To address these concerns, Intrusion Detection Systems (IDS) have become indispensable for protecting IoT networks. These systems employ sophisticated techniques, including machine learning, to detect potential threats at an early stage. The effectiveness of IDS is closely tied to the optimization of the features used for detecting intrusions. Techniques such as Principal Component Analysis (PCA), Genetic Algorithms (GA), and various dimensionality reduction methods are essential for improving detection accuracy while reducing computational demands. Research indicates that numerous learning models have been developed to enhance IoT network efficiency and threat detection. As IoT technology continues to advance, the creation of robust, adaptable, and efficient IDS will be crucial for preserving the security and integrity of these interconnected networks. Future research should focus on developing models that can accurately identify session types—whether normal or intrusive—without relying on prior information.

REFERENCES

1. R. Vinayakumar, M. Alazab, S. Srinivasan, Q. V. Pham, S. K. Padannayil, and K. Simran, “A visualized botnet detection system based deep learning for the internet of things networks of smart cities,” IEEE Transactions on Industry Applications, vol. 56, pp. 4436–4456, 2020.
2. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, “Deep learning approach for intelligent intrusion detection system,” IEEE Access, vol. 7, pp. 41525–41550, 2019.
3. Smith S. IoT Connections to Reach 83 Billion by 2024, Driven by Maturing Industrial Use Cases. Accessed Apr. 2020;10:2021.
4. Awotunde J.B., Chakraborty C., Adeniyi A.E. Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection. Wirel. Commun. Mob. Comput. 2021;2021:7154587. doi: 10.1155/2021/7154587.
5. Wazzan M., Algazzawi D., Albeshri A., Hasan S., Rabie O., Asghar M.Z. Cross Deep Learning Method for Effectively Detecting the Propagation of IoT Botnet. Sensors. 2022;22:3895. doi: 10.3390/s22103895.
6. Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Rep. 2021;7:8176–8186. doi: 10.1016/j.egyr.2021.08.126.
7. Wani, A., Revathi, S.: Analyzing threats of IoT networks using SDNbased intrusion detection system (SDIoT-IDS). Commun. Comput. Inf.Sci. 828, 536–542 (2018).
8. Valdivieso Caraguay, ÁL., et al.: SDN: Evolution and Opportunities inthe Development IoT Applications. Int. J. Distrib. Sens. Netw. 10(5),735142(2014).
9. Kiani, F.: A survey on management frameworks and open challenges inIoT. Wirel. Commun. Mob. Comput. 1–33 (2018).
10. Xiu Kan, Yixuan Fan, Zhijun Fang, Le Cao, Neal N. Xiong, Dan Yang, Xuan Li. "A novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization Convolutional Neural Network", Information Sciences, Volume 568, 2021, Pages 147-162.
11. Fatani, A.; Dahou, A.; Abd Elaziz, M.; Al-qaness, M.A.A.; Lu, S.; Alfadhli, S.A.; Alresheedi, S.S. Enhancing Intrusion Detection Systems for IoT and Cloud Environments Using a Growth Optimizer Algorithm and Conventional Neural Networks. Sensors 2023, 23, 4430.
12. Saied, M., Guirguis, S. & Madbouly, M. A Comparative Study of Using Boosting-Based Machine Learning Algorithms for IoT Network Intrusion Detection. Int J Comput Intell Syst 16, 177 (2023)
13. Zambare, P., Liu, Y. (2024). An Optimized Graph Neural Network-Based Approach for Intrusion Detection in Smart Vehicles. In: Puthal, D., Mohanty, S., Choi, BY. (eds) Internet of Things. Advances in Information and Communication Technology. IFIPIoT 2023. IFIP Advances in Information and Communication Technology, vol 683. Springer, Cham.

14. Kalyanam, L.K., Joshi, R., Katkoori, S. (2024). Layer-Wise Filter Thresholding Based CNN Pruning for Efficient IoT Edge Implementations. In: Puthal, D., Mohanty, S., Choi, BY. (eds) Internet of Things. Advances in Information and Communication Technology. IFIPIoT 2023. IFIP Advances in Information and Communication Technology, vol 683. Springer, Cham.
15. T. -T. -H. Le, R. W. Wardhani, D. S. C. Putranto, U. Jo and H. Kim, "Toward Enhanced Attack Detection and Explanation in Intrusion Detection System-Based IoT Environment Data," in IEEE Access, vol. 11, pp. 131661-131676, 2023, doi: 10.1109/ACCESS.2023.3336678.
16. K. A. Awan, I. Ud Din, M. Zareei, A. Almogren, B. Seo-Kim and J. A. Pérez-Díaz, "Securing IoT With Deep Federated Learning: A Trust-Based Malicious Node Identification Approach," in IEEE Access, vol. 11, pp. 58901-58914, 2023, doi: 10.1109/ACCESS.2023.3284677.
17. The rest of this article is organized as follows. Section II provides an overview of work done by other researchers in field of IOT intrusion detection. Section III describes our methodology for the proposed model, including the feature clustering model, and learning model. Section IV describes the evaluation results and analyzes the current state of the art. Finally, Section V concludes this article.
18. M. Mohy-Eddine, A. Guezzaz, S. Benkirane, M. Azrour and Y. Farhaoui, "An Ensemble Learning Based Intrusion Detection Model for Industrial IoT Security," in Big Data Mining and Analytics, vol. 6, no. 3, pp. 273-287, September 2023.
19. Fatani, M. Abd Elaziz, A. Dahou, M. A. A. Al-Qaness and S. Lu, "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization," in IEEE Access, vol. 9, pp. 123448-123464, 2021, doi: 10.1109/ACCESS.2021.3109081.
20. Ullah I., Mahmoud Q.H. (2020) A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In: Goutte C., Zhu X. (eds) Advances in Artificial Intelligence. Canadian AI 2020.