Research Journal of Engineering Technology and Medical Sciences (ISSN: 2582-6212), Volume 07, Issue 04, December-2024
Available at www.rjetm.in/

Advanced Strategies for Detecting and Preventing IoT Botnet Attacks: Integrating VAEs and Network-Based Approaches

[1]Babli Arjunwar, [2]Dr. Vivek Sharma, [3]Balwant raghuvanshi

[1]M. Tech Scholar, Department of Computer Science and Engineering, Technocrats institute of Technology, Bhopal, MP, India.

[2]Head of Department, Department of Computer Science and Engineering, Technocrats institute of Technology, Bhopal, MP, India

[3]Associate Professor, Department of Computer Science and Engineering, Technocrats institute of Technology, Bhopal, MP, India

[1]babliarjunwar88890@gmail.com , [2]sharma.vivek95@yahoo.in, [3]balwant8336@gmail.com

Abstract: *The rapid expansion of the Internet of Things (IoT) has revolutionized connectivity but has simultaneously introduced critical cybersecurity vulnerabilities, particularly through botnet attacks. This review explores the evolving threat landscape in IoT ecosystems and proposes an integrated defense strategy combining signature-based and anomaly-based detection techniques. Central to this approach is the use of Variational Autoencoders (VAEs), a form of unsupervised machine learning that enhances predictive modeling and threat detection. The paper categorizes botnet architectures into star, multiple-server, hierarchical, and random topologies, explaining their operational mechanisms and vulnerabilities. Emphasis is placed on the effectiveness of network-based detection strategies, including anomaly detection methods that establish behavioral baselines, and signature-based systems capable of identifying known attack patterns. Additionally, the study highlights the limitations of these traditional techniques in identifying zero-day and encrypted threats. A novel contribution of the paper is its inclusion of machine learning and deep learning techniques, which demonstrate high accuracy in detecting both known and emerging threats. The research draws on real-world case studies, including the adoption of embedded SIM (eSIM) technology, to illustrate adaptive connectivity management and predictive threat modeling. The integration of industry insights, such as those from leading cybersecurity firms, enriches the proposed framework. The review underscores the need for hybrid and scalable models that can evolve alongside the dynamic nature of IoT deployments. Conclusively, it advocates for proactive, AI-driven approaches to secure IoT networks, ensuring resilience against increasingly complex cyber threats.*

Keywords: *IoT security, botnet attacks, Variational Autoencoders (VAEs), anomaly detection, signature-based detection, embedded SIM (eSIM), cloud computing security.*

I. INTRODUCTION

The widespread presence of Internet of Things (IoT) devices has garnered significant interest, since they have expanded into an extensive network of embedded systems that can access the internet. Notwithstanding all of the benefits, there are drawbacks to the increased use of IoT, most notably security flaws and the possibility of malware attacks. IoT networks are seriously at risk from the increasingly sophisticated botnet attacks [1]. We urgently need to take proactive actions against these risks in light of recent incidents like the 2021 'biggest botnet'[2]. This study explores how botnet assaults affect Internet of Things devices and suggests a network-based detection and prevention method that uses algorithms based on anomaly and signature detection.

The main goal of this research is to improve the security of data transmission in cloud computing environments, ultimately protecting the networked devices that are essential to modern industries, and to develop a predictive model utilizing Variational Autoencoders (VAEs) to forecast and analyze IoT security threats, with a particular focus on botnet attacks. The technique aims to accomplish these goals by drawing inspiration from the creative approaches used by leading companies in the field, such Palo AltoNetworks, to tackle the security difficulties associated with IoT devices [3]. This study also takes into account the results of Kaleido Intelligence, which highlights the changing IoT landscape by projecting a sharp increase in the use of embedded SIM (eSIM) technology for IoT applications [4]. The establishment of Trident IoT, a technology and engineering firm dedicated to expediting the time-to-market for connected products and optimizing RF development, underscores the increasing significance of effectively integrating IoT technologies [5]. One common method of integrating IoT devices is to use embedded SIM (eSIM) technology. Because they can be programmed and are remote provisioning capability, eSIMs are especially well-suited to the ubiquitous and dynamic nature of Internet of Things deployments. eSIM configurations depending on consumption patterns can be optimized by the examination of connectivity patterns in Internet of Things device data. This adaptive connectivity management ensures that resources are used efficiently and affordably. This research aims to contribute to the creation of prediction models that can effectively manage IoT security threats by taking these real-world difficulties and industry trends into account. The primary objective is to enhance data transmission security within cloud computing environments, thereby safeguarding the interconnected devices integral to contemporary industries. A predictive model employing Variational Autoencoders (VAEs) is developed to forecast and analyze IoT security threats, with a particular emphasis on botnet attacks. This approach draws inspiration from innovative solutions implemented by leading cybersecurity firms addressing IoT security challenges.

In addition to addressing security concerns, the study considers the evolving landscape of IoT connectivity, notably the increasing adoption of embedded SIM (eSIM) technology. eSIMs offer programmable and remotely provisioned capabilities, aligning well with the dynamic nature of IoT deployments. By analyzing connectivity patterns in IoT device data, eSIM configurations can be optimized based on consumption patterns, ensuring efficient and cost-effective resource utilization. This adaptive connectivity management is crucial for the seamless integration and operation of IoT technologies.

By integrating these real-world challenges and industry trends, this research contributes to the development of predictive models capable of effectively managing IoT security threats. The proposed framework aims to provide a robust defense mechanism against botnet attacks, ensuring the resilience and reliability of IoT networks in an increasingly connected world.

II. IOT BOTNETS AND ARCHITECTURES

Four forms of botnet architecture are distinguished: hierarchical, random, multiple-server, and star topologies. [6]. As illustrated in Figure 1, the centralized botnet, sometimes referred to as star topology, is the most widely used and swiftly spreading kind of botnet. An attack is started when a bot master posts a command to the control-and-command server, which then sends the command to every bot. Once the bots receive the command, the attack will commence with the attack pattern that the bot master has set. An Internet service provider or researcher can discover and use the control-and-command server, which is the foundation of this architecture, to successfully take down a botnet. [7-8] if the link between the control-and-command servers is broken, the bots cannot receive commands from the bot master, which will stop the attack. The number of control-and-command servers varies from the star topology in many server architectures. Because of how easily things might go wrong, the many servers' topology modifies the configurations of the control-and-command servers.[9]

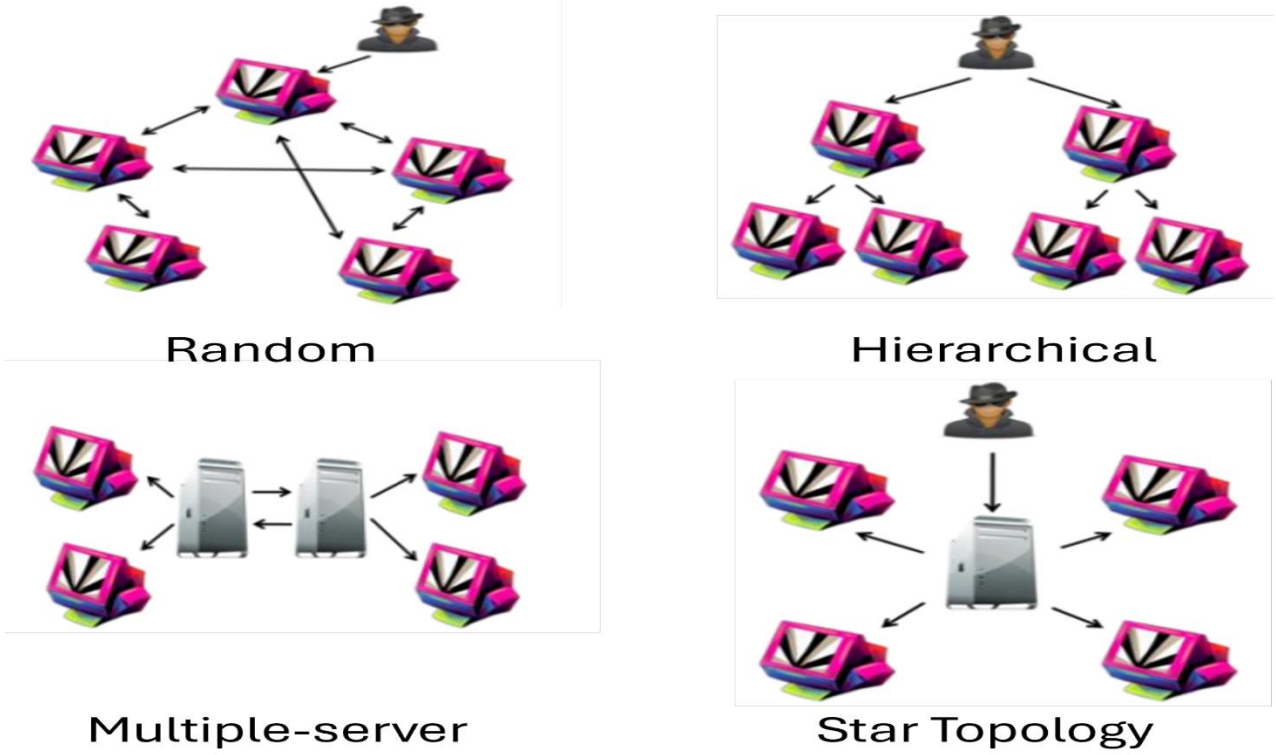

Figure 1. Botnet architecture

Figure 1 illustrates the four primary types of botnet architectures—Random, Hierarchical, Multiple-server, and Star Topology—each representing different strategies for command and control in malicious networks. In the Random topology, every infected device (bot) can communicate with multiple others, forming a peer-to-peer (P2P) structure that enhances resilience and obfuscation, as there is no central control server. The Hierarchical architecture organizes bots in tiers, where upper-level bots relay commands from the botmaster to lower levels, offering concealment and fault tolerance. The Multiple-server model employs several command-and-control (C&C) servers, allowing redundancy and increased robustness; if one server fails or is taken down, others maintain control over the botnet. Lastly, the Star Topology (or centralized model) features a single C&C server distributing commands to all bots, which simplifies control but creates a single point of failure. Each topology reflects varying balances of efficiency, scalability, and vulnerability, influencing how botnet threats operate and how they must be defended against.

Every control-and-command server in the network is set up to send out commands. The botnet will continue to operate as planned even if one of the servers is discovered and malfunctions; another server will take its place. The bot master states

that the attack will go on as long as one of the command-and-control servers is operational [30]. There are some shortcomings with the multiple-server architecture. The bot master believes that building a multiple-server botnet is more challenging due to its intricacy when compared to a star topology. The hierarchical botnet shown in Figure 1 does not require a control-and-command server because it consists of several high-level bots. High-level bots are used as a C&C server in order to conceal the bot master and C&C server furtherIt is challenging to eliminate a botnet that is constructed with a hierarchical design by the bot master because of the C&C server's defenses [10–11]. The botnet only loses some of its bot population if the high-level bot is found. The architecture of a random botnet is shown in Figure 1. As can be seen in Figure 1, the random botnet is devoid of a command-and-control server. When a bot receives commands from the bot master, it will relay them to other bots that are connected to it. Because every bot is perceived as a C&C server, a random botnet has strong security despite being very difficult to deploy. One of the main issues with the centralized botnet is locating and destroying the command and control servers. The C&C server in the P2P botnet is extremely difficult to find because each bot serves as a C&C server, so if one of the bots in a random topology botnet's architecture is discovered, its impacts are limited and cannot bring down the entire network [12].

III. IOT SECURITY VULNERABILITIES AND BOTNET/DDOS ATTACKS

The security architecture of the Internet of Things (IoT) is the focus of many research, where the entire system is divided into four distinct layers—the application layer, network layer, device layer, and service/application support layer—each with its own set of security concerns [13]. These layers reflect the functional and operational complexity of IoT environments, and vulnerabilities at any of these levels can compromise the entire system. There is general agreement among these investigations that security flaws vary depending on the tier. For example, while the application layer is prone to data manipulation and injection attacks, the device layer often suffers from inadequate hardware-based security protections due to resource constraints. Even though various researchers have put forth various IoT security architecture models [14], they all concur that no single IoT model can provide the best possible protection against all kinds of threats. This limitation arises from the heterogeneous and dynamic nature of IoT devices and protocols, making it difficult to standardize a universal defense model.

Specifically, there are numerous security risks that can affect the Internet of Things (IoT) network layer, such as DoS attacks, Sybil attacks, Man-in-the-Middle (MiTM) attacks, and selective forwarding [15]. The network layer is particularly vulnerable because it is responsible for the data transmission between devices, often over untrusted or public communication channels. Attackers can exploit these channels to intercept, alter, or reroute data flows, thereby compromising the confidentiality, integrity, and availability of IoT services. Among these different kinds of attacks, botnets and DDoS attacks elicit the greatest focus, perhaps due to the potential impact of such attacks in terms of compromising the availability of information systems [16]. These attacks can disrupt large-scale operations, take critical services offline, and cause significant economic damage, making them a top priority for researchers and cybersecurity professionals working in the IoT domain.

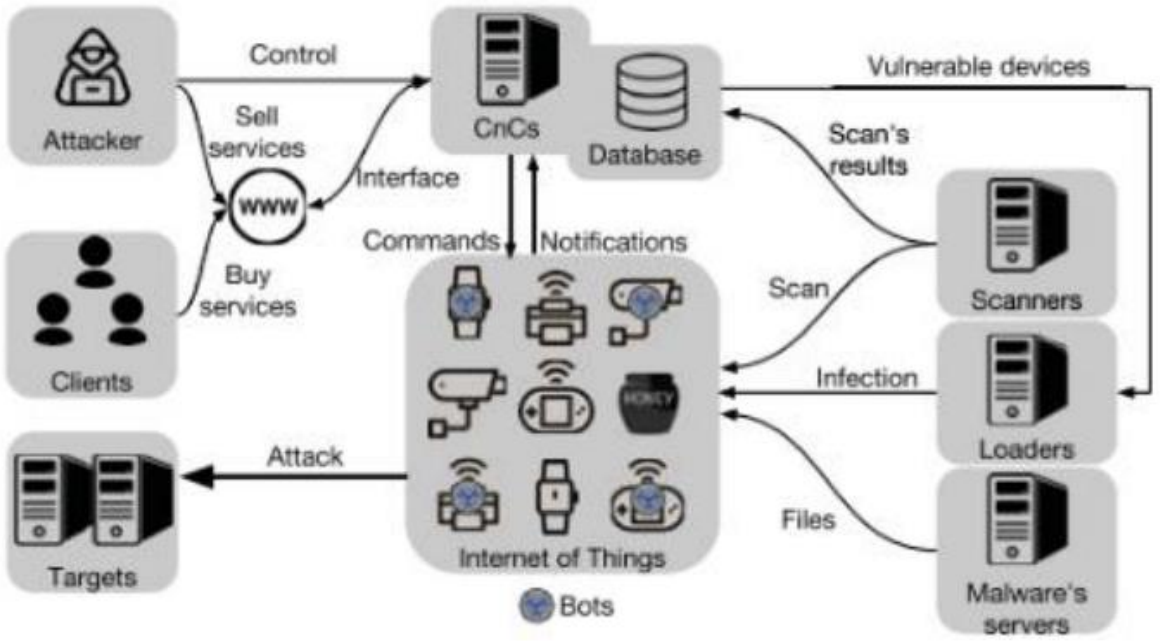

Figure 2. Typical IoT botnet ecosystem [17]

Figure 2 illustrates a typical Internet of Things (IoT) botnet ecosystem, depicting the flow of control and interaction among various components involved in a botnet attack. The process begins with the attacker, who controls the Command and Control (CnC) servers and can also sell or offer botnet services through the WWW to interested clients. The scanners are used to identify vulnerable IoT devices, and the results of these scans are stored in a database. Once vulnerable devices are detected, loaders exploit these devices by injecting malware obtained from malware servers, turning them into bots. These bots—represented by IoT devices like cameras, sensors, and smart appliances—are then controlled via commands from the CnC servers. They receive notifications and are mobilized to launch attacks on selected targets (e.g., servers or networks). The attackers can orchestrate attacks such as DDoS, data theft, or system disruption through these compromised devices. This architecture highlights the commercial nature of botnets (via client interfaces), the automation of device compromise, and the seamless control attackers maintain over widespread IoT-based botnets.

A typical Internet of Things botnet ecosystem consists of databases, malware servers, scanners for probing devices, loaders for logging into vulnerable devices, bots or infected devices, scanners for probing devices, and loaders for controlling the botnet (See Figure 2) [17]. The following are a few instances of the most common assaults made against IoT systems:

A. Denial of Service (DoS): Due to enormous cyber-attacks IoT systems or network resources become unreachable to the intended authorized users. The purpose of these attacks is to temporarily or permanently interrupt the services provided by a host IoT system.

B. Distributed Denial-of-Service (DDoS): A distributed DDoS attack is a malicious network attack that interrupts systematic traffic and network services. It involves overwhelming the target or neighboring infrastructure with a disproportionate volume of network traffic. DDoS attacks are effective when attackers exploit various compromised systems to produce a huge volume of traffic in the network. IoT systems or other devices which are the part of the network can also be targeted with these attacks.[18]

C. Marai Botnet Attack: Cybercriminals employ the software known as Mirai to turn networked devices into remotely controlled robots in a catholic scale network as a part of botnet. It primarily targets internet consumer electronics, including IP cameras and routers for the house. Mirai was frequently used as an initiator in attacks like DoS/DDoS.

D. Sybil Attack: Peer-to-peer networks are vulnerable to attacks by Sybil. A Sybil attack modifies the IoT device's identity in order to produce multiple anonymous identities and consume excessive power. It was named after Sybil in remembrance of Sybil, the author of the book Sybil, which follows a woman dealing with dissociative identity disorder. The network access granted by reputation systems is often compromised by an IoT device in a multi-identity network. Sybil attacks leverage this IoT system network vulnerability to initiate early attacks.[19]

IV. NETWORK BASED DETECTION TECHNIQUES

The network based solution is a better way to protect the IOT devices and network from these devastating cyber-attacks. The network-based detection techniques, which serve as a frontline defense mechanism for identifying malicious activity in IoT ecosystems, are broadly categorized into three primary types.

A. Anomaly-Based Detection Method involves monitoring the regular behavior of network traffic and establishing a baseline profile for each device within the network. Any notable deviation from this baseline is flagged as an anomaly, which could indicate a potential security threat [20]. This method is particularly effective in identifying previously unseen attacks that do not match known signatures. It is further subdivided into two core approaches:

- Statistics-Based Detection: This technique utilizes statistical models to define the normal behavior of the network. It then continuously compares incoming traffic against this model to identify deviations that might suggest an intrusion. These methods are grounded in mathematical analysis, such as calculating mean, variance, and standard deviation of network metrics to detect outliers and irregular patterns in data flows.
- Knowledge-Based Detection Method: This method relies on a repository of known behaviors or patterns, developed through extensive testing under various scenarios. When network behavior deviates from this established knowledge base, an anomaly is flagged. It is especially useful in environments where historical data is available for establishing reliable behavioral baselines [21].
- Machine Learning Techniques: Machine learning (ML) has become a crucial component in the evolution of botnet detection strategies. As a subset of Artificial Intelligence (AI), ML enables systems to autonomously learn and make decisions without being explicitly programmed for every scenario. In the context of botnet detection, ML models are trained to distinguish between benign and malicious network traffic. This includes both supervised learning, where models learn from labeled datasets, and unsupervised learning, which identifies patterns and anomalies in unlabeled data. These techniques are increasingly favored due to their adaptability, scalability, and ability to uncover complex attack vectors that traditional methods might overlook [22–23].

B. Signature-Based Detection Techniques

In order to identify and stop a known botnet in the future, a unique identifier is created for it using signature-based approaches, also known as intrusion detection systems. One of the main shortcomings of signature-based detection systems is their inability to identify zero-day attacks, or attacks for which there is no corresponding signature in the repository. Nevertheless, these techniques are effective on established botnet features or characteristics [24].

The signature-based detection method's primary flaw is that it can only identify known threats for which the rules are stored in its rules database. However, the stateful protocol-based detection techniques are only partially able to examine encrypted data. Nonetheless, the examination of traffic behavior, or anomaly detection, is highly successful in identifying undiscovered threats as well as analyzing encrypted traffic [24–25]. The machine learning methodology has demonstrated exceptional performance in anomaly detection methods in recent years In order to identify and discern between the patterns and behaviors of legitimate and malicious traffic, machine learning-based detection techniques are trained on datasets. From this point forward, the machine learning models are helpful in identifying new botnet and DDoS attacks that are derivatives or copies of the current botnet and DDoS attacks by analyzing the patterns of both normal and attack traffic. Once IOT devices are infected with malware and begin executing harmful actions under the control of a botmaster, the botnet is detected by the current methods for detecting botnet attacks. Additionally, the majority of machine learning-based botnet detection models now in use are only as good as the datasets they were trained on [25].

One study highlighted the challenges of deploying NIDS in industrial and robotic systems, emphasizing the need for specialized solutions in these environments [26]. Another review provided a taxonomy of ML methods for intrusion detection, discussing the strengths and weaknesses of each approach [27]. Further, a comprehensive overview of IDS technologies examined both traditional methods and recent advancements, offering insights into their applicability in modern network environments [28]. The application of ML algorithms in IDS, especially within IoT networks, has been explored, showcasing various supervised, unsupervised, and semi-supervised learning techniques [29]. A systematic literature review focused on ML-based intrusion detection in IoT, particularly addressing Distributed Denial of Service (DDoS) attacks, and highlighted the dominance of certain datasets and models in achieving high accuracy [30]. Another study reviewed anomaly-, signature-, and hybrid-based approaches, providing a comprehensive overview of the state of the art in network IDS [31]. The integration of ML and DL approaches in intrusion detection and prevention has been extensively reviewed, emphasizing the need for hybrid systems that can adapt to modern network threats [32]. A systematic review of hybrid intrusion detection systems further underscored the importance of combining different methodologies to enhance detection accuracy [33]. In the context of software-defined networks (SDN), the design of NIDS based on ML has been demonstrated, showcasing the use of various tree-based techniques for attack detection [34]. Furthermore, the potential of large language models (LLMs) in labeling NIDS rules with MITRE ATT&CK techniques has been investigated, comparing their performance with traditional ML models [35]. Lastly, a deep learning model combining attention mechanisms and bidirectional long short-term memory (Bi-LSTM) networks has been proposed to address issues of low detection accuracy in NIDS [36]. These studies collectively demonstrate the evolving landscape of NIDS, highlighting the shift towards more intelligent, adaptive, and transparent systems. The continuous refinement of ML and DL models, along with the development of hybrid and explainable frameworks, underscores the commitment to advancing network security in the face of evolving cyber threats.

TABLE 1 Comparative Analysis of Network-Based Intrusion Detection Studies

Ref. No.	**Study Focus**	**Key Techniques**	**Application Area**	**Advantages**	**Limitations**
[26]	NIDS in industrial and robotic systems	Context-specific adaptations	Industrial, Robotics	Tailored for robotics/industry	Limited generalizability
[27]	Taxonomy of ML methods for intrusion detection	Taxonomic ML classification	General Networks	Clear method classification	Doesn't cover hybrid methods
[28]	Overview of IDS technologies	Traditional + modern IDS comparison	General Networks	Broad insight into IDS evolution	Lacks experimental validation
[29]	ML algorithms in IoT IDS	Supervised, unsupervised, semi-supervised	IoT Networks	Diverse ML strategy coverage	May need large labeled datasets

[30]	ML-based IDS in IoT for DDoS detection	Dataset and model performance analysis	IoT Networks	Focus on real attack types	Focused on specific attack type
[31]	Anomaly, signature, and hybrid IDS approaches	Comparative IDS types	General Networks	Comprehensive strategy analysis	No performance metrics included
[32]	Integration of ML and DL in IDS	Hybrid ML-DL systems	General Networks	Adaptive and intelligent detection	Complex model integration
[33]	Systematic review of hybrid IDS	Multi-technique fusion	General Networks	Enhanced accuracy via fusion	Potential implementation complexity
[34]	ML-based NIDS in SDN	Tree-based ML algorithms	Software Defined Networks	Effective in SDN scenarios	Specific to SDN only
[35]	LLMs vs ML for labeling NIDS rules	LLMs and MITRE ATT&CK	General Networks	Higher semantic detection accuracy	LLMs require large computing power
[36]	Attention + Bi-LSTM for NIDS	Attention and Bi-LSTM model	General Networks	Improved detection on imbalanced data	Resource intensive

Table 1 presents a comparative analysis of 11 recent studies (Ref. [26]– [36]) focused on network-based intrusion detection systems (NIDS), highlighting diverse methodologies, application domains, and their relative strengths and weaknesses. Each study explores a specific focus area ranging from industrial-specific NIDS to advanced deep learning integrations for general and IoT networks. Techniques employed vary from taxonomic classifications and supervised machine learning to hybrid ML-DL systems and attention-based neural networks. Application areas span from general enterprise networks and software-defined networks (SDN) to specialized IoT and robotic environments. The advantages include domain-specific adaptability, enhanced detection accuracy, and improved handling of complex threats, while limitations range from scalability and generalizability issues to the high computational demands of deep learning models. This comparative overview underscores the shift towards intelligent, adaptive detection systems, while also revealing ongoing challenges in creating universally robust and resource-efficient IDS solutions.

V. Integrating VAEs with Network-Based Strategies

The integration of Variational Autoencoders (VAEs) with network-based intrusion detection systems (NIDS) has emerged as a promising approach for real-time botnet detection in IoT environments. VAEs, known for their capability to learn latent representations of data, can effectively model the normal behavior of network traffic, enabling the detection of anomalies indicative of botnet activities. For instance, a study proposed a hybrid model combining VAEs with one-class classifiers to detect botnets by analyzing network traffic data flows, achieving satisfactory performance in identifying malicious activities [37] Another research introduced a Recurrent Variational Autoencoder (RVAE) model that captures sequential characteristics of network traffic, demonstrating robustness in detecting botnets in streaming data [38]. Effective feature engineering and preprocessing are critical for enhancing the performance of VAE-based detection systems. Techniques such as normalization, dimensionality reduction, and selection of relevant features can significantly impact the model's ability to distinguish between benign and malicious traffic. A study emphasized the importance of latent space dimension in VAE models, revealing that appropriate dimensionality can improve detection performance in IoT botnet scenarios [39]. Additionally, research highlighted the use of communication graphs to represent device behavior, offering a novel perspective for feature extraction in IoT networks [40]. Several studies have demonstrated the efficacy of Variational Autoencoder (VAE)-based hybrid systems for botnet detection across diverse IoT environments. One study successfully utilized VAEs to differentiate between benign and malicious traffic, achieving high accuracy in IoT botnet detection by learning low-dimensional representations of normal behavior [41]. Another investigation addressed the challenge of class imbalance by integrating VAE with cost-sensitive learning techniques, resulting in lightweight models

that maintained robust performance despite skewed data distributions [42]. Similarly, the N-BaIoT model combined network-based behavior snapshots with deep autoencoders, showcasing a scalable and accurate approach to detecting IoT botnet activity [43].

For environments with limited labeled data, researchers proposed a hybrid autoencoder-based model that maintained reliable detection rates despite small-sample constraints [44]. In the realm of real-time detection, VAEs were applied to model probabilistic distributions in network traffic, enabling efficient and continuous anomaly identification [45]. Expanding on hybrid methods, one study merged CNN and LSTM architectures with flow-based features, yielding improved botnet classification performance by leveraging both spatial and temporal patterns [46]. Deep learning techniques have also evolved with architectures like Bidirectional LSTM autoencoders, which proved effective for capturing sequential data in IoT botnet traffic, further enhancing detection accuracy [47]. Another study evaluated the impact of latent space dimensions on detection performance, finding that VAE encoders outperformed Vision Transformer-based encoders in certain configurations [48]. A novel approach using Recurrent VAEs was introduced to exploit temporal dynamics in network traffic for botnet detection, demonstrating superior adaptability to streaming data [49]. Finally, research focusing on learning latent space representations reaffirmed the potential of VAE models in capturing distinguishing features of IoT network behavior for accurate botnet identification [50].

Table 2 Comparative Analysis of VAE-Based Hybrid Systems for IoT Botnet Detection

Ref. No.	**Study Focus**	**Technique Used**	**Application Domain**	**Feature Approach**	**Model Strength**	**Limitation**	**Outcome**
[39]	Latent space dimensionality in VAEs	Dimensionality tuning in VAEs	IoT botnet detection	Latent space representation	Improved detection sensitivity	May require tuning for each dataset	Higher performance with optimal dimensions
[40]	Communication graphs for device behavior	Graph-based feature extraction	IoT traffic analysis	Device behavior modeling	Novel feature perspective	Complexity in real-time graph updates	Enhanced interpretability
[41]	VAE for differentiating benign/malicious traffic	Standard VAE	General IoT environment	Low-dimensional representation	High accuracy for labeled datasets	Limited adaptability to new attack types	Reliable initial anomaly detection
[42]	Cost-sensitive VAE for imbalanced datasets	VAE + cost-sensitive learning	IoT botnet detection	Imbalance-aware features	Robustness with skewed data	May underperform on balanced datasets	Lightweight and scalable
[43]	N-BaIoT using deep autoencoders	Deep autoencoder (NIDS)	IoT behavioral analysis	Snapshot extraction	Scalable and accurate	Dataset-specific tuning needed	Proven effectiveness across devices
[44]	Intrusion detection with small-sample problem	Hybrid autoencoder	Limited training data	Minimal labeled data	Maintains detection in low-data scenarios	May miss subtle anomaly patterns	Practical in constrained data settings
[45]	Real-time anomaly detection with VAEs	VAE for streaming network traffic	Live traffic monitoring	Probabilistic modeling	Real-time adaptability	Resource-intensive for high-speed networks	Continuous detection with low latency
[46]	Flow-based detection using CNN + LSTM	CNN + LSTM hybrid model	Botnet traffic analysis	Temporal-spatial flow features	Captures complex traffic patterns	Computational overhead	Enhanced classification precision

[47]	Bi-LSTM Autoencoder for sequential data	Bidirectional LSTM Autoencoder	IoT traffic logs	Sequential traffic patterns	Accurate sequence learning	High training complexity	Boosted detection accuracy
[48]	VAE vs Vision Transformer encoder	VAE & ViT encoder comparison	IoT detection framework	Comparative latent encoding	Demonstrates VAE's strengths	ViT better in some visual domains	Validated VAEs for network anomaly tasks
[49]	Recurrent VAE for sequential traffic	Recurrent Variational Autoencoder (RVAE)	Streaming botnet traffic	Temporal feature learning	Suitable for streaming detection	Needs optimized recurrent layer configuration	Effective on evolving patterns
[50]	Latent space learning with VAEs	VAE latent space optimization	General IoT security	Discriminative latent vectors	Strong anomaly separation	Less interpretability of latent features	Accurate IoT botnet identification

VI. CONCLUSION

The increasing proliferation of Internet of Things (IoT) devices has introduced a new era of interconnected convenience but also exposed networks to a wider surface area for cyber-attacks, particularly in the form of botnets. This review has comprehensively examined the multifaceted security challenges that arise within the IoT ecosystem, focusing primarily on the growing threat posed by sophisticated and adaptive botnet attacks. These attacks exploit vulnerabilities across all layers of the IoT architecture—device, network, application, and support—disrupting services and compromising data integrity. The review underscores the insufficiency of traditional intrusion detection methods, especially against evolving and zero-day threats, thus reinforcing the need for advanced detection frameworks. In addressing these challenges, the paper introduces a dual-layered detection strategy that integrates anomaly-based and signature-based methods to create a robust network-based detection system. Central to the proposed methodology is the incorporation of Variational Autoencoders (VAEs), which serve as powerful tools for modeling normal traffic behavior and identifying deviations that may indicate botnet activity. The study also highlights the strategic importance of emerging technologies such as embedded SIM (eSIM) for adaptive connectivity management and cloud security enhancement. Furthermore, the role of machine learning, particularly supervised and unsupervised techniques, is emphasized for their ability to automate and improve detection accuracy over time. By drawing on real-world industry practices and synthesizing recent academic findings, this paper lays a foundational framework for the development of predictive, scalable, and intelligent IoT security systems. Future research should focus on refining these models, ensuring they remain adaptive to dynamic environments, and validating their effectiveness across diverse real-world datasets. Ultimately, proactive integration of VAEs with network-based strategies represents a critical step toward safeguarding the future of IoT infrastructures.

REFERENCES

[1] Detection of Botnet in the IoT Network Syeda Lamiya Mumtaz, ITM Web of Conferences 63, 01019 (2024) https://doi.org/10.1051/itmconf/20246301019.
[2] R. Lakshmanan, "Researchers Uncover 'Pink' Botnet Malware That Infected Over 1.6 Million Devices." Accessed: Nov. 14, 2023. [Online].
[3] Predicting IoT Botnet Attacks for Enhanced Data Transmission Security in the Cloud Using Variational AutoencodersChandrasekar Venkatachalam, IJISAE, 2024, 12(20s), 820–828.
[4] R. Daws, "'Qiang Huang, Palo Alto Networks: On Addressing IoT Device Security Challenges.' Internet of things news. IoT tech News, August 16, 2023". Available at: https://www.iottechnews.com/news/2023/aug/16/qiang-huang-palo-alto-networks-iot-device-security-challenges/.
[5] [4]R. Daws, "'Kaleido Intelligence Forecasts ESIM Adoption Surge for IoT.' Internet of things news. IoT tech News, August 21, 2023". Available at: https://www.iottechnews.com/news/2023/aug/21/kaleido-intelligence-forecasts-esim-adoption-surge-iot/.
[6] [5]R. Daws, "'Z-Wave Alliance Celebrates Trident IoT's Launch.' Internet of things news. IoT tech News, August 17, 2023". Available at: https://www.iottechnews.com/news/2023/aug/17/z-wave-alliance-celebrates-trident-iot-launch/
[7] Gelgi M, Guan Y, Arunachala S, Samba Siva Rao M, Dragoni N. Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. Sensors. 2024; 24(11):3571. https://doi.org/10.3390/s24113571.

[8] Zhu, Z.; Lu, G.; Chen, Y.; Fu, Z.J.; Roberts, P.; Han, K. Botnet Research Survey. In Proceedings of the 2008 32nd Annual IEEE International Computer Software and Applications Conference, Turku, Finland, 28 July–1 August 2008; pp. 967–972. [Google Scholar] [CrossRef]
[9] Liu, C.Y.; Peng, C.H.; Lin, I.C. A survey of botnet architecture and batnet detection techniques. Int. J. Netw. Secur. 2014, 16, 81–89. [Google Scholar]
[10] Dittrich, D.; Dietrich, S. P2P as botnet command and control: A deeper insight. In Proceedings of the 2008 3rd International Conference on Malicious and Unwanted Software (MALWARE), Alexandria, VA, USA, 7–8 October 2008; pp. 41–48. [Google Scholar] [CrossRef]
[11] Imam, M.; Nir, M.P.; Matrawy, A. A Survey on Botnet Architectures, Detection and Defences. Int. J. Netw. Secur. 2014, 17, 264–281. [Google Scholar].
[12] Survey for Anomaly Detection of IoT Botnets Using Machine Learning Auto-Encoders Reem Alhajr, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 10 (2019) pp. 2417-2421.
[13] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-mariona, "IoDDoS — The Internet of Distributed Denial of Service Attacks : A Case Study of the Mirai Malware and IoT-Based Botnets IoDDoS — The Internet of Distributed Denial of Service Attacks A Case Study of the Mirai Malware and IoT-Based Botnets," no. April 2017.
[14] "OWASP IoT Top 10 2018," OWASP Internet of Things Project, 12-Apr-2019. [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of _Things_Project#tab=OWASP_IoT_Top_10_2018_Mapping_Project.
[15] A. Marzano et al., "The Evolution of Bashlite and Mirai IoT Botnets," 2018 IEEE Symp. Comput. Commun., pp. 813–818, 2018.
[16] A. Lohachab and B. Karambir, "Critical Analysis of DDoS — An Emerging Security Threat over IoT Networks," vol. 3, no. 3, 2018.
[17] Enhancing IoT Security with Deep Stack Encoder using Various Optimizers for Botnet Attack Prediction Archana Kalidindi, Vol. 14, No. 6, 2023.
[18] D. Li, L. Deng, M. Lee, and H. Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," Int. J. Inf. Manage., vol. 49, pp. 533-545, Dec 2019.
[19] P. I. R. Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the Internet of Things: Challenges, threats and solutions," Internet Things, vol. 5, pp. 41-70, Dec 2019.
[20] Two-Fold Machine Learning Approach to Prevent and Detect IOT BOTNET Attacks Ms.M.Sandhya Vani, Volume 07, Issue 02, Feb 2023 ISSN 2581 – 4575.
[21]] B. K. Dedeturk and B. Akay, ``Spam _ltering using a logistic regression model trained by an arti_cial bee colony algorithm," Appl. Soft Comput., vol. 91, Jun. 2020, Art. no. 106229.
[22] N. Vlajic and D. Zhou, ``IoT as a land of opportunity for DDoS hackers," Computer, vol. 51, no. 7, pp. 26_34, 2018.
[23] GitHub Survived Biggest DDoS Attack Ever Recorded. Accessed: May 3, 2021. [Online]. Available: https://github.blog/2018-03-01- ddosincident- report/
[24] A Literature Survey on IoT Botnet Detection Techniques Umar Maikudi, 4 th International Conference on Information Technology in Education and Development 2021.
[25] Oladipupo, Esau Taiwo, Abikoye Oluwakemi Christianah, Akande Noah Oluwatobi, Kayode Anthonia Aderonke, Adeniyi Jide Kehinde (2020), "Comparative Study of Two Divide and Conquer Sorting Algorithms: Quicksort and Mergesort", Procedia Computer Science, 171, pp 2532–2540. https://doi.org/10.1016/j.procs.2020.04.274.
[26] Holdbrook, Richard & Odeyomi, Olusola & Yi, Sun & Roy, Kaushik. (2024). Network-Based Intrusion Detection for Industrial and Robotics Systems: A Comprehensive Survey. Electronics. 13. 10.3390/electronics13224440. http://dx.doi.org/10.3390/electronics13224440
[27] Vanin, Patrick & Newe, Thomas & Dhirani, Lubna Luxmi & O'Connell, Eoin & O'Shea, Donna & Lee, Brian & Rao, Muzaffar. (2022). A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning. Applied Sciences. 12. 11752. 10.3390/app122211752. http://dx.doi.org/10.3390/app122211752
[28] Diana, Lorenzo & Dini, Pierpaolo & Paolini, Davide. (2025). Overview on Intrusion Detection Systems for Computers Networking Security. Computers. 14. 87. 10.3390/computers14030087. http://dx.doi.org/10.3390/computers14030087
[29] Mohammed, Mazin & Alothman, Hasanien. (2024). Using Machine Learning Algorithms in Intrusion Detection Systems: A Review. Tikrit Journal of Pure Science. 29. 63-74. 10.25130/tjps.v29i3.1553. http://dx.doi.org/10.25130/tjps.v29i3.1553
[30] Bankó, Márton & Dyszewski, Szymon & Králová, Michaela & Limpek, Márton & Papaioannou, Maria & Choudhary, Gaurav & Dragoni, Nicola. (2025). Advancements in Machine Learning-Based Intrusion Detection in IoT: Research Trends and Challenges. Algorithms. 18. 209. 10.3390/a18040209. http://dx.doi.org/10.3390/a18040209
[31] Abdulganiyu, Oluwadamilare & Ait Tchakoucht, Taha & Saheed, Yakub. (2023). A systematic literature review for network intrusion detection system (IDS). International Journal of Information Security. 22. 10.1007/s10207-023-00682-2. http://dx.doi.org/10.1007/s10207-023-00682-2
[32] Abraham, Jitti & V R, Bindu. (2021). Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches: A Review. 1-4. 10.1109/ICAECA52838.2021.9675595. http://dx.doi.org/10.1109/ICAECA52838.2021.9675595

[33] Alhasan, Seiba & Abdul-Salaam, Gaddafi & Missah, Yaw & Anisi, Mohammad. (2024). HYBRID NETWORK INTRUSION DETECTION SYSTEMS: A SYSTEMATIC REVIEW. 1-35.
[34] Alzahrani, Abdulsalam & Alenazi, Mohammed. (2021). Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks. Future Internet. 13. 111. 10.3390/fi13050111. http://dx.doi.org/10.3390/fi13050111
[35] Daniel, Nir & Kaiser, Florian & Giladi, Shay & Sharabi, Sapir & Moyal, Raz & Shpolyansky, Shalev & Murillo, Andres & Elyashar, Aviad & Puzis, Rami. (2025). Labeling Network Intrusion Detection System (NIDS) Rules with MITRE ATT&CK Techniques: Machine Learning vs. Large Language Models. Big Data and Cognitive Computing. 9. 23. 10.3390/bdcc9020023. http://dx.doi.org/10.3390/bdcc9020023
[36] Fu, Yanfang & Du, Yishuai & Cao, Zijian & Li, Qiang & Xiang, Wei. (2022). A Deep Learning Model for Network Intrusion Detection with Imbalanced Data. Electronics. 11. 898. 10.3390/electronics11060898. http://dx.doi.org/10.3390/electronics11060898
[37] Snoussi, R., Youssef, H. VAE-Based Latent Representations Learning for Botnet Detection in IoT Networks. J Netw Syst Manage 31, 4 (2023). https://doi.org/10.1007/s10922-022-09690-4
[38] Kim, J., Sim, A., Kim, J., & Wu, K. (2020, December). Botnet detection using recurrent variational autoencoder. In GLOBECOM 2020-2020 IEEE global communications conference (pp. 1-6). IEEE. https://doi.org/10.48550/arXiv.2004.00234
[39] Wasswa, H., Nanyonga, A., & Lynar, T. (2024, March). Impact of Latent Space Dimension on IoT Botnet Detection Performance: VAE-Encoder Versus ViT-Encoder. In 2024 3rd International Conference for Innovation in Technology (INOCON) (pp. 1-6). IEEE. https://doi.org/10.48550/arXiv.2504.14879
[40] Muñoz, D. C., & Valiente, A. D. C. (2023). A novel botnet attack detection for IoT networks based on communication graphs. Cybersecurity, 6(1), 33. https://doi.org/10.1186/s42400-023-00169-6
[41] U., Om & Pranavi, Dharmala & Laxmi, B. & R., Devasena. (2022). Variational Autoencoder for IoT Botnet Detection. 10.4018/978-1-6684-6444-1.ch005. http://dx.doi.org/10.4018/978-1-6684-6444-1.ch005
[42] Wasswa, Hassan & Lynar, Timothy & Abbass, Hussein. (2025). Enhancing IoT-Botnet Detection using Variational Auto-encoder and Cost-Sensitive Learning: A Deep Learning Approach for Imbalanced Datasets. 10.48550/arXiv.2505.01437. http://dx.doi.org/10.48550/arXiv.2505.01437
[43] Meidan, Yair & Bohadana, Michael & Mathov, Yael & Mirsky, Yisroel & Shabtai, Asaf & Breitenbacher, Dominik & Elovici, Yuval. (2018). N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. IEEE Pervasive Computing. 17. 12-22. 10.1109/MPRV.2018.03367731. http://dx.doi.org/10.1109/MPRV.2018.03367731
[44] Wei, Nan & Yin, Lihua & Tan, Jingyi & Ruan, Chuhong & Yin, Chuang & Sun, Zhe & Luo, Xi. (2023). An Autoencoder-Based Hybrid Detection Model for Intrusion Detection With Small-Sample Problem. IEEE Transactions on Network and Service Management. PP. 1-1. 10.1109/TNSM.2023.3334028. http://dx.doi.org/10.1109/TNSM.2023.3334028
[45] Gate, Bill. (2025). Variational Autoencoders for Real-Time Anomaly Detection in Network Traffic: Toward Self-Learning Intrusion Detection Systems.
[46] Asadi, M., Heidari, A. & Jafari Navimipour, N. A New Flow-Based Approach for Enhancing Botnet Detection Efficiency Using Convolutional Neural Networks and Long Short-Term Memory. Knowl Inf Syst (2025). https://doi.org/10.1007/s10115-025-02410-9
[47] Wasswa, H., Nanyonga, A., & Lynar, T. (2024, March). Impact of Latent Space Dimension on IoT Botnet Detection Performance: VAE-Encoder Versus ViT-Encoder. In 2024 3rd International Conference for Innovation in Technology (INOCON) (pp. 1-6). IEEE. https://doi.org/10.48550/arXiv.2504.14879
[48] Snoussi, Ramzi & Youssef, Habib. (2022). VAE-Based Latent Representations Learning for Botnet Detection in IoT Networks. Journal of Network and Systems Management. 31. 10.1007/s10922-022-09690-4. http://dx.doi.org/10.1007/s10922-022-09690-4
[49] Bai, T., Li, Y., Wang, Y. et al. A Hybrid VAE Based Network Embedding Method for Biomedical Relation Mining. Neural Process Lett 55, 81–92 (2023). https://doi.org/10.1007/s11063-021-10454-5
[50] Lin, J., Lei, H., & Michailidis, G. (2024). A VAE-based Framework for Learning Multi-Level Neural Granger-Causal Connectivity. arXiv preprint arXiv:2402.16131. https://doi.org/10.48550/arXiv.2402.16131