Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DEVELOPING AUTONOMOUS CYBER DEFENCE SYSTEMS USING AI-DRIVEN INTRUSION DETECTION FOR IOT NETWORKS

BAHA ELDIN HAMOUDA[1]

[1]Department of Information Technology, Gulf Colleges, Hafar Al-Batin, Saudi Arabia

E-mail: [1]bahahamouda@yahoo.com, bhh@gulf.edu.sa

ABSTRACT

As the Internet of Things (IoT) continues to grow exponentially, securing interconnected devices against evolving cyber threats has become paramount. This paper explores the development of an autonomous cyber defence system leveraging artificial intelligence (AI) to enhance intrusion detection for IoT networks. Traditional security measures fall short in resource-constrained, heterogeneous environments like IoT. Hence, we propose an AI-driven Intrusion Detection System (IDS) capable of real-time threat detection and autonomous response. Using a hybrid machine learning approach and reinforcement learning for automated mitigation, the system is evaluated on publicly available IoT security datasets. Results demonstrate improved detection accuracy, reduced false alarms, and efficient resource utilization. This research contributes to the advancement of intelligent, self-governing security mechanisms in IoT ecosystems.

Keywords: *Autonomous Cyber Defence, AI-Driven Intrusion Detection, Internet of Things (IoT) Security, Machine Learning for Cybersecurity, Intelligent Network Protection.*

1. INTRODUCTION

The Internet of Things (IoT) provides platform interconnecting all physical devices, sensors, actuators, and software systems. Such interconnection will allow communication and decision-making with intelligence [1]. With billions of connected devices around the globe, IoT has a significant role to play in multiple industries such as healthcare, transportation, agriculture, smart cities, and manufacturing [2].

The even more rapid proliferation of IoT applications has cast complexity and heterogeneity to unprecedented levels upon the network infrastructure. Devices diverge vastly in terms of capabilities, operating systems, and communication protocols. Therefore, in combination with limitations as far as computational resources are concerned and the absence of security mechanisms on a standard basis, IoT systems appear to be vulnerable on a wider range of cyber threats.

Cybercriminals have taken advantage of the increased number of IoT devices to expand their attack surface. Unlike traditional computing environments, the IoT networks consist of mostly low-powered devices that are extremely hard to update and secure [3]. As a result, these devices become vulnerable to any threat due to weak authentication, hardcoded passwords, insecure firmware, and absence of encryption. Attackers have often been seen exploiting these vulnerabilities to initiate distributed denial-of-service (DDoS) attacks, steal data, spoof, or propagate botnets [4].

The decentralized nature of IoT systems allows single-compromise devices to be used as an entry point for attackers into the entire network [5]. Instances like the Mirai botnet attack demonstrated the destructive power of coordinated cyberattacks using IoT, with thousands of infected devices brought together to incapacitate major internet services. The fallout of such breaches ranges from enormous financial losses and disruption of operations to actual endangerment of human lives in vital systems such as healthcare and smart transportation [6].

Traditional cybersecurity systems, often designed for centralized and well-resourced environments, find themselves in an awkward fit for IoT ecosystems [7]. They are simply not agile, scalable, or intelligent enough to counter dynamic, large-scale, and stealthy attacks. This creates an urgent demand for new security paradigms that can accurately detect and autonomously respond-in-real-time to threats.

Manual or reactive cybersecurity approaches are no longer realizable in such complexities and magnitudes as modern IoT networks. The defence strategies against IoT systems must also function autonomously, make decisions with minimal human intervention, and adapt to the ever-evolving threat landscape [8]. This is especially pertinent with the need for real-time intrusion detection and mitigation in mission-critical environments, where any delay in threat response could induce catastrophic ramifications.

On the contrary, autonomous cyber defence solutions promise to bridge this divide through intelligent detection with automated response [9]. Such a system would need to analyse very large data quantities, detect malicious activity, and carry out appropriate countermeasures without interfering with legitimate operations or activities. Such promising scenarios can be best accomplished with the aid of artificial intelligence (AI) and machine-learning (ML)-based systems [10].

AI-based intrusion detection systems work by using machine learning algorithms to detect anomalies and threats based on learning the patterns from historical and real-time network data [11]. Leveraging past experiences, the AI system can identify anomalies and threats; in contrast to signature-based IDS that depend on the use of predefined signatures corresponding to certain threats, it can easily identify new or zero-day attacks through behavioural analysis and classification techniques [12]. Deep learning models based on CNN (Convolutional Neural Networks) and LSTM (Long Short-Term Memory) have proven particularly effective in dealing with time-dependent data that highly entangles with complex environmental parameters generated by IoT devices. AI integrated with an autonomous decision-making framework such as reinforcement learning equips the systems to detect as well as dynamically respond to threats [13]. The systems can isolate compromised devices, block malicious traffic, and adapt any defence mechanism over time, adding to the resilience of the IoT infrastructures.

This research aims to develop a comprehensive and autonomous cyber defence system tailored for IoT networks using AI-driven intrusion detection techniques. The core objectives of the study are:

- To evaluate the effectiveness of various AI/ML algorithms for detecting IoT-specific cyber threats
- To design a real-time intrusion detection architecture that integrates with IoT environments.
- To implement autonomous response mechanisms using reinforcement learning for proactive defence.
- To validate the performance of the proposed system using real-world datasets and practical deployment scenarios

The major contribution that this research makes lies in its integrative approach between detection and response, through AI, in bringing forth a scalable, adaptive, and autonomous security framework concerning the rapidly changing landscape of IoT.

2. LITERATURE REVIEW

2.1 IoT Network Architecture and Security Challenges

Designated as a major development in connectivity, the IoT is a system for interconnection of physical objects that are also equipped with sensors, software, and networking capabilities for autonomous data collection and exchange mention [14]. IoT architectures typically consist of three layers: the perception layer (sensors and actuators), the network layer (gateways and communication protocols), and the application layer (data processing and services) [15]. By providing a layered setup, it intends to provide seamless integration of heterogeneous devices in distinct contexts: for example, healthcare, industrial automation, smart homes, and transportation systems [16].

A major characteristic of IoT networks is the heterogeneity. Devices may differ from each other in terms of hardware platforms, operating systems, network interfaces, and communication protocols (e.g., Zigbee, MQTT, CoAP, 6LoWPAN) [17]. Such aspects of heterogeneity make it difficult to design a common security model, for rarely can a common solution be applied [18].

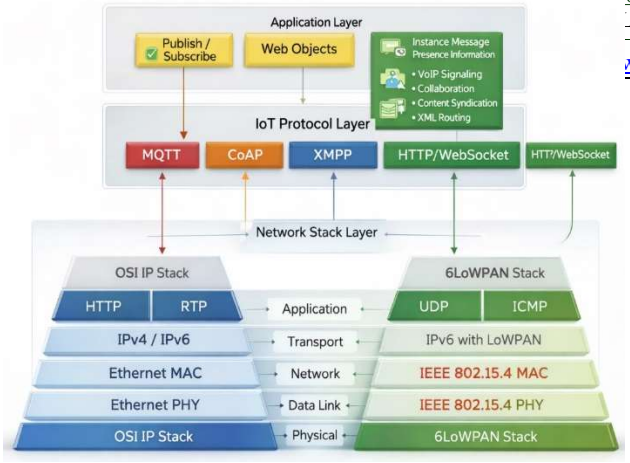

Figure 1: IoT Infrastructure

Figure 1 shows the layered infrastructure of the IoT. This representation shows integration across various communication protocols, network stacks, and application services. MQTT, CoAP, XMPP, and HTTP/WebSocket are some of the lightweight communication protocols. They are supported by network stacks like TCP/IP and 6LoWPAN. This network stack is primarily used in low-power networks. XML and JSON are some of the data formats. There are various security vulnerabilities.

IoT presents unique challenges stemming from its scale of deployment. Wired and wireless sensors and actuators together are estimated in the tens of billions of their interconnectivity by 2025. Any of the traditional centralized security mechanisms are hardly workable to provide real-time surveillance and protection-throughout such large networks [19]. Scalability, thus, becomes an important requirement for any security solution meant to work in IoT environments.

Another major limitation is due to resource limitation. Many IoT devices operate with limited processing power, memory, and energy resources. These constraints limit the implementation of sophisticated cryptographic protocols or real-time monitoring agents on the device level [20]. Security, therefore, has to be offloaded more often to edge or gateway devices, which themselves may be under threat.

2.2 Common Attack Vectors in IoT Networks

IoT networks are becoming increasingly fragile against a variety of cyber threats, both new and old, owing to their pervasive deployment, heterogeneous architecture, and often limited on-service inbuilt security [21]. The Distributed Denial of Service (DDoS) attacks, are overwhelmingly quite common and disruptive types of attacks where illegitimate traffic overloads devices or networks, depriving services from legitimate users [22]. An example of such hijacking and orchestrating a major DDoS attack over global infrastructure is the famous Mirai botnet attack in 2016, which attacked several IoT devices worldwide, from IP cameras to home routers by exploiting weak or default log-in credentials [23].

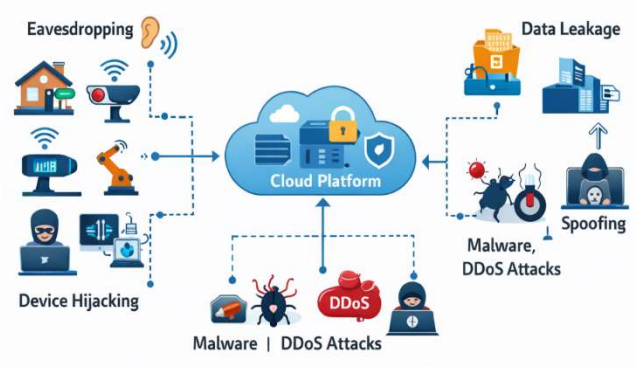

Figure 2: IoT attack types and vulnerabilities [24]

Figure 2 shows a layered taxonomy of attack vectors that can be utilized to attack IoT devices. Level 1 concerns network attacks that affect communication, including DoS, DDoS, and MitM attacks. Level 2 concerns direct attacks on IoT devices, including physical, side-channel, and firmware attacks. Level 3 concerns attacks on users at the application level, including malware, data manipulation, and breaking access control. The layered approach shows the complexity of securing IoT devices and the need for multiple layers of security.

Spoofing and impersonation are common threats, especially in IoT environments. Malicious actors impersonate trusted devices or users to gain unlawful access to sensitive data or network functions [25]. No single strong or standardized authentication mechanism exists across many IoT platforms; therefore, spoofing attacks are comparatively easy to carry out and can grant unauthorized control of devices or what is even worse, can result in leakage of data. Weak, hardcoded passwords and open ports are just some security settings that make IoT devices attractive targets for botnet builders [26].

Man-in-the-Middle (MitM) attacks are among the major threats IoT networks in themselves suffer. Attackers intercept communications between IoT devices and backend servers, thereby allowing manipulation or passive eavesdropping on the transmitted data [27]. This leaves the door open to successful MitM attacks, especially with the many lightweight communication protocols in use in IoT, most of them not using adequate encryption or authentication [28]. This vulnerability is especially

critical in applications involving control systems, such as industrial IoT or smart home environments where data integrity is vital for operational safety.

2.3 Traditional Intrusion Detection Systems (IDS)

2.3.1 Signature-Based vs. Anomaly-Based Systems

These systems are now the basic development units of the architecture of cybersecurity. They can be anything, from monitoring network traffic to system activity, for malicious behaviour detection, violations of policy, or indications of compromises, such as user ongoing activities [29]. IDS are essentially classified into two broad categories: signature-based detection systems or anomaly-based detection systems. IDS types have their merits and demerits depending on their applications in dynamic resource-constrained environments such as IoT [30].

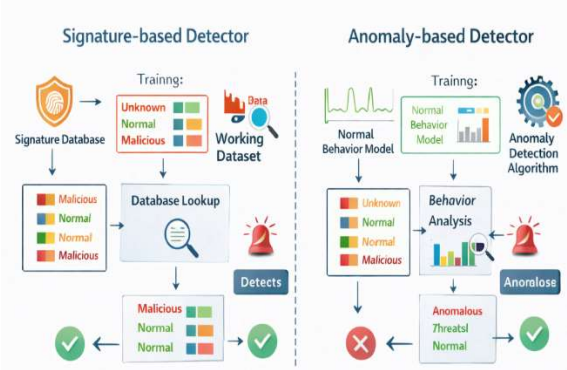

Figure 3: Signature vs. anomaly-based detection comparison [31]

Figure 3 compares two types of IoT security detection mechanisms: signature-based and anomaly-based. Signature-based detection is very effective at identifying known threats with a low false-positive rate, but it cannot detect unknown threats, also known as zero-day threats. Anomaly-based detection is effective at identifying unknown threats, but it comes with a high rate of false positives and requires constant model tuning.

Signature-based IDS detect intrusions by the use of precompiled set match databases (signatures) of known threats by their one-to-one mapping on an activity of the network. Signature basically is the fingerprint or pattern of a previous attack, that is, a specific byte sequence, traffic pattern, or even a system call sequence. This approach works efficiently and quite accurately for previously familiar threats and has low rates of false positives owing to its deterministic nature. The main problem associated with signature-based intrusion detection systems is that they cannot detect new or metamorphic threats, such as zero-day vulnerabilities and polymorphic malware [32]. Moreover, signature maintenance and that of the entire signature database have to be executed over a large number of IoT devices. This brings in logistical and performance-related challenges [33].

Anomaly-based IDS aim to solve this problem by understanding what constitutes "normal" behaviour for that particular system or network and then flagging deviations from this as possible threats [30]. The detection of new forms of attacks previously unseen before can dynamically change the profile of the threat as the adaptive behaviour sample feature tries to encompass the varied and changing environment present in dynamic scenarios. It is relatively impossible, however, to create a general and specific enough baseline in IoT environments, where aspects such as highly diversified device behaviours are normally considered context-sensitive [34]. Thus, they generally have a much higher churn in terms of false positives because they tend to mistake benign but unusual activity as bad behaviour [35]. The learning, modelling, and continuous analysis of behaviour, coupled with processing demand, adds severe stress to the very limited processing and memory capability of IoT devices.

2.3.2 Limitations in Dynamic and Resource-Constrained Environments

Due to these challenges, the traditional Intrusion Detection Systems (IDSs) cannot meet the performance or efficiency requirements for use in IoT networks. One of the major issues is the extreme resource constraints that are typical of IoT devices [36]. In contrast with servers or desktop workstations, the IoT endpoints have very minimal computing power and memory that sometimes is measured in kilobytes and with very low energy budget. Thus, the deployment of traditional IDSs, which are resource-intensive and architected for powerful hardware, is certainly not optimal for these devices [37]. Installing a full-fledged IDS agent on every single IoT node is neither practical nor economically feasible, particularly in large-scale deployments such as smart cities or industrial IoT networks.

Another major hurdle for conducting threat analysis is the dependency on centralized architecture. In most traditional cases of IDS deployment, the network traffic is diverted to centralized servers for the actual data analysis and detection of anomalies [38]. Such a model converts the analysis into a time-consuming process and is

harmful where IoT applications are concerned. In applications such as Remote Patient Monitoring, autonomous vehicles, or industrial automation, a few seconds delay in declaring an attack, may well lead to catastrophes of great consequence: either a massive operational failure or a safety hazard. Therefore, real-time detection and response imply that the edge or distributed IDS architecture should be highly capable of functioning with minimal delay.

Devices often connect and disconnect, and functional behaviour can change depending on temporal, spatial, or contextual conditions. For example, smart lighting during the night might behave differently than during the day. Anomaly-based IDS systems that depend on static behavioural models come unstuck in such environments and are quickly outdated, leading to false positives or misses [39]. But adaptation is continuously required as device behaviour evolves, yet this is difficult to achieve in a traditional IDS setting.

One more hindrance is the absence of standardization for IoT communication protocols. Conventionally, enterprise networks use protocols that are fairly anodyne, whereby most of the work is carried out using HTTP, TCP/IP, or DNS [40]. In contrast, IoT networks tend to use lightweight and special-purpose protocols such as Zigbee, MQTT, CoAP, or Bluetooth Low Energy (BLE). Most of the existing IDSs in this field are protocol-based and focused on monitoring one or just a few selected protocols, whereas traffic outside of their design consideration lies beyond the monitoring scope [41]. The heterogeneous nature of protocols presents an obstacle for the deployment of universal IDS solutions and incites the need for detection systems that are more flexible and context-aware.

Likewise, several interrelated constraints make obvious the necessity for an urgent push toward next-generation IDS technologies that would be lightweight and adaptive with decentralized deployment capabilities [42]. There are exciting developments in the area of AI-based IDS frameworks, which are believed to raise the prospects of scalability, contextual awareness, and real-time threat detection in diverse environments.

2.4 AI in Cybersecurity

Machine Learning and Deep Learning have emerged as transformative techniques in intrusion detection and The ability to really stand out for artificial intelligence in discovering complex non-linear patterns into very large data sets, the key aim of which would be served extremely well by AI [43]. Unlike older traditional intrusion detection systems that relied mostly on present rules or signatures, one built on AI can learn from both historical and real-time network data and hence detect both known and unknown forms of malicious behaviour. The learning-based methods allow detection capabilities for a wide range of very subtle anomalies, adaptive threat patterns, and zero-day attacks, which have evaded the conventional detection mechanisms [44].

Within machine learning, several algorithms have demonstrated their applicability in developing useful IDS models. An example would be Support Vector Machines commonly used on binary classification problems for separating normal from malicious traffic with distinct decision boundaries [45]. However, its performance is heavily dependent on kernel choice and hyperparameter tuning, both of which can occasionally be very costly in terms of computational resources. Random Forest therefore is quite appreciated in terms of robustness, resistance to overfitting, and interpretation, which is an ensemble learning technique aggregating predictions from numerous decision trees with differing perspectives [46]. The K-Nearest Neighbours (KNN) algorithm is a simple and efficient method under low dimensional conditions, yet it faces extreme difficulty in terms of scalability and computation in high-dimensional datasets [47], which are common in the IoT networks. Naive Bayes (NB) is a probabilistic classifier based on Bayes' theorem. This classifier works well for high-dimensional datasets even as it presupposes the independence of features, a condition that does not always hold true in real-world antivirus data.

Deep learning algorithms enhance the abilities of AI-based IDS through an automatic extraction of various hierarchical features within the raw input data [48]. Artificial Neural Networks (ANNs) are quite versatile in modelling non-linear decision boundaries and are generally utilized in supervised learning scenarios. CNNs are made for the detection of spatial patterns from structured network data, e.g. packet matrices or encoded flow data [49]. Recurrent Neural Networks (RNNs), especially in the form of Long Short-Term Memory (LSTM), are intended and greatly suited for analysing time-dependent sequences, such as traffic logs or system call traces, maintaining the timing dynamics of attacks. In an unsupervised scenario, Autoencoders learn to reconstruct normal behaviour and flag anomalies by measuring reconstruction error; this technique is quite light and simple for anomaly detection.

Together, these AI tools engender higher levels of detection accuracy, adaptability to the changing nature of threats, and an ability to generalize to

unseen attack vectors, qualities of utmost importance in the dynamic and heterogeneous environments of IoT networks.

2.5 Previous Work on AI-Driven IDS for IoT

The deployment of AI into the Intrusion Detection Systems of IoT networks has become a hot topic in recent years. Many works have discussed how to improve IDS through ML and DL algorithms regarding accuracy, adaptability, and effective use against security threats in resource-limited and heterogeneous IoT spaces. Though the studies do deliver candid contributions, critical examination would unveil the limitations that still hinder the evolution of fully autonomous and scalable cyber defence systems [50].

Applied deep learning models, namely CNNs and RNNs, on the NSL-KDD dataset for the identification of IoT traffic for malicious behaviours. Their work showed that deep learning models tended to outperform their traditional ML antecedents such as the SVM and Decision Tree in terms of detection accuracy and adaptability. The authors pointed out that their findings, when applied in a real-world setting, could be challenged by the use of generic datasets like NSL-KDD, which fail to encompass the full scale of diversity over IoT protocols and attack types.

Likewise [51], proposed a distributed deep neural network (DNN)-based approach that decentralized training among IoT devices. Their method countered communication overhead in centralized learning and improved intrusion detection performance. By doing so, however, they assume a certain level of computation exists at the edge, which may not be the case for many low-power IoT nodes. Their approach did enhance detection rates, but they still did not have autonomous response features and therefore depended on a manual intervention post-alert.

N-BaIoT, introduced by [52], employed unsupervised anomaly detection using autoencoders in smart home environments. The model effectively captured deviations from normal device behaviour and accomplished an impressive detection accuracy of above 99%. Although it efficiently detected compromised devices, the framework shows passive operation without the ability to autonomously contain or remediate any observed threats. Autonomy is a deficiency that most contemporary AI-driven IDS frameworks share. The intrusion detection capability is also based on the edge [53]. Devised lightweight neural networks tailored to resource-constrained IoT environments. Their solution determined that even the lowest power devices could contribute to detection of threats at the network edge. Nonetheless, the system's inflexibility to varied attack patterns was due to its reliance on static thresholds and manual tuning. Besides, in its performance measure, the system kept varying results on different datasets, thus lowering its performance in a real-world heterogeneous IoT environment. Other approaches have integrated such hybrid systems which combine signature- detection methods with AI-based anomaly detection in order to exploit both detection methods' strengths. While hybrid systems improve detection coverage, they tend to increase complexity and resource requirements that may not align with the constraints of IoT networks.

2.6 Gaps in Existing Approaches: Lack of Autonomy, Explainability, and Adaptability

With autonomy in AI-enabled IDS being a critical gap in current research endeavours, although the detection accuracy can be said to be considerably high, very few have consciously developed decision-making paradigms that would trigger responses toward real-time threats. Other than being under-researched, autonomous defence systems with reinforcement learning and policy-based action selection mechanisms have yet to form the basis of any concrete validation. The next emerging challenge is explainability. The black box paradigm of deep learning models renders them accurate yet untrustworthy as stakeholders in safety-critical domains (healthcare, autonomous vehicles) seek interpretable outputs to trust system decisions. Research into Explainable AI (XAI) for IDS is still very much in its infancy. Adaptability is still limited. Many IDS are trained offline with static datasets that do not reflect the ever-changing nature of real-world threats. Over time, models will lose their relevance or efficacy, called model drift. Continuous learning or online learning mechanisms are needed to sustain effectiveness within a dynamic environment. Finally, problems regarding scalability and deployment feasibility still exist. Where cloud-based solutions hold the computation power, they introduce latency and privacy concerns. Edge-based AI appears to be a way forward, but this requires lightweight and energy-efficient models, which is not yet fully developed.

3. PROBLEM STATEMENT AND RESEARCH QUESTIONS

3.1 Problem Statement

The fast spread of IoT devices across many sectors, including healthcare, smart homes, and industrial control systems, is adding tremendously to the already big digital attack surface [1].

Heterogeneity, scalability, limited computational power, and a mélange of communication protocols are the peculiar traits of IoT networks. Given these characteristics, the traditional security methods like conventional Intrusion Detection Systems (IDS) are rendered largely incapable of efficaciously protecting the IoT environments [2].

Most of the existing IDS solutions are passive, concentrating solely on intrusion detection without any capacity for autonomous response or real-time mitigation. Moreover, many AI-based implementations of IDS are built on generalized datasets or customized to a specific use case, thereby limiting their scalability and adaptability across various IoT ecosystems [3]. There are the issues regarding latency in centralized data processing and the diminished feasibility to run resource-heavy models on resource-constrained edge devices.

In this juxtaposition of threat scenario against the IoT infrastructure, where threats such as DDoS, spoofing, and botnet infiltration keep changing and evolving, there is an utmost need for an intelligent, lightweight, and autonomous IDS system that could detect and respond to security threats in real time with minimal human intervention [4]. The use of AI, especially ML, and DL offers a way forward in this direction for IDS. However, so far, the literature has not yet explored optimizing these AI techniques for autonomous real-time cyber defence in resource-limited heterogeneous IoT environments.

3.2 Research Questions

To address this overarching challenge, the research is guided by the following comprehensive and interrelated questions:

- How can AI techniques be optimized to enable accurate, real-time intrusion detection in heterogeneous and resource-constrained IoT networks?
- Which machine learning and deep learning models demonstrate the highest efficacy in identifying IoT-specific attack vectors such as spoofing, botnet infiltration, and DDoS attacks?
- What design principles and architectures can support the integration of reliable, autonomous response mechanisms within AI-driven IDS to minimize human dependency and latency in threat mitigation?
- How can these AI-driven IDS frameworks be generalized to ensure scalability, interoperability, and resilience across different IoT applications and communication protocols?

4. METHODOLOGY

4.1 Data Collection and Preprocessing

For training and evaluation purposes, there were employed two common datasets, namely UNSW-NB15 and Bot-IoT, to propose and develop an AI-based autonomous Intrusion Detection System (IDS) for IoT networks. The selection of these datasets was because they describe in detail benign and malicious behaviours that directly affect the IoT environment. The UNSW-NB15 dataset involves modern intrusions such as reconnaissance, fuzzers, and shellcode attacks, while the Bot-IoT dataset relates to IoT situations and has detailed samples of botnet activity, DDoS attacks, and data theft attempts.

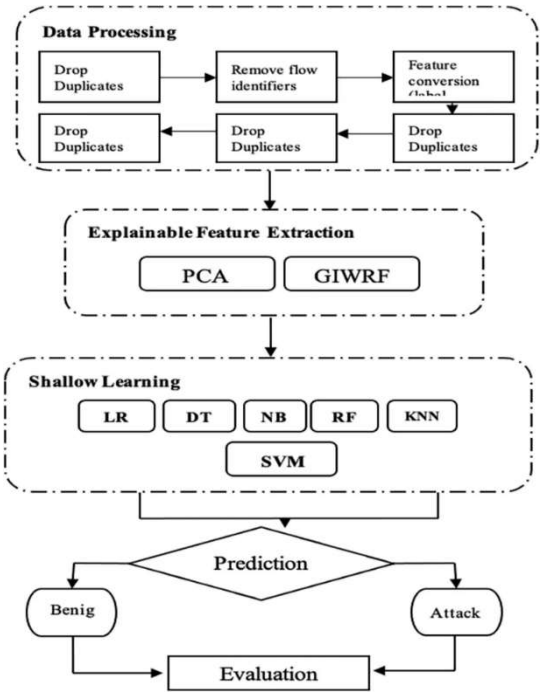

Figure 4: Proposed Framework

Before training the model, the data underwent significant preprocessing. First, irrelevant and redundant features were eliminated using correlation-based feature selection, which computes Pearson correlation coefficients to eliminate attributes exhibiting low variance or high inter-feature redundancy. This way, only the most informative attributes are retained for training, reducing training complexity and enhancing model generalizability.

Next, all numeric features were normalized using Min-Max scaling to a scale of [0,1]. The

normalization is crucial-as CNN and LSTM algorithms are sensitive to input scales-for convergence during training and maintaining relative proximity among data points. Categorical variables were also encoded using one-hot encoding to maintain numerical compatibility for learning algorithms. After preprocessing, the datasets were split into training (70%), validation (15%), and testing (15%) subsets through stratified sampling to maintain the class distribution in each split.

4.2 Model Design

The detection model is designed as a hybrid deep learning architecture that incorporates some of the best features of the Convolution Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks for effective feature extraction and temporal pattern recognition. The CNN part of this model serves as the very first step in the model pipeline, taking normalized input features into a series of convolutional layers that capture some spatial correlations and hierarchical patterns present within the data. The extracted features are then flattened and passed to the LSTM layer, which captures sequential dependencies and time-based trends in network behaviour-an essential ingredient in spotting sophisticated and evolving IoT attacks like botnet propagation or slow-scan techniques.

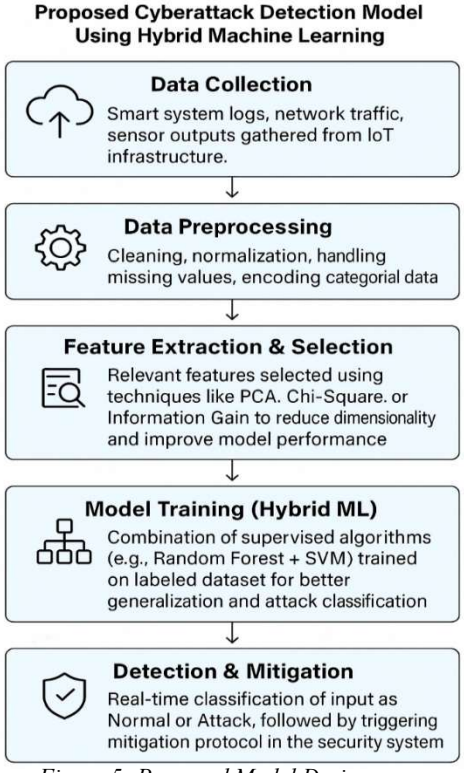

Figure 5: Proposed Model Design

After the LSTM layer, the output is sent to a Random Forest (RF) classifier. This ensemble model was chosen for its good resistance to overfitting, high interpretability, and good performance even with noisy or partially informative features. The deep learning-ensemble learning combination accomplishes accuracy and generalization-the specific challenge of variances and the evolving nature of IoT traffic patterns. Hyperparameter tuning for all models was then done through Bayesian optimization on the validation set to achieve optimal architecture depth, learning rates, number of estimators (for RF), and batch sizes.

4.3 Autonomous Response Mechanism

Besides intrusion detection, the system consists of an autonomous response layer based on RL-Reinforcement Learning or Q-learning. The environment is modelled as a Markov Decision Process- MDP- where the agent observes the state of the network (for instance, detection status, the affected node, and type of attack) and picks the best action from a predefined list. In this case, the actions include: (1) isolation of infected nodes from the network, (2) rerouting critical traffic away from compromised traffic segments, and (3) generating automated alerts to system administrators using MQTT-based messaging.

The Q-learning agent is trained using the simulation episodes generated from attack patterns in these datasets. A reward structure is set up to encourage behaviours aimed at minimizing system damage and maintaining service availability while penalizing false positives or ineffective mitigations. The agent learns a policy over several iterations that maps observed states into fitting responses, thus facilitating the process of autonomous mitigation without constant human supervision. It also saves its decisions into a policy table, periodically updated through online refinement in the live environment.

4.4 System Architecture

The suggested architecture is designed in a simulated edge-cloud culture to capture real IoT deployments. The detection elements are distributed among edge nodes, where initial classification by lightweight CNN-LSTM models is performed with negligible latency. This would typically be in embedded devices or edge gateways with limited computing capabilities, such as those based on Raspberry Pi or Jetson Nano platforms. Once a potential threat is identified, an anomaly summary is relayed via MQTT to streamline a deeper analysis in the centralized cloud nodes while coordinating a multi-node response through the trained agent RL.

The cloud layer possesses visibility into the network globally and administers the distributed RL policy. This dual-launched deployments enable real-time threat detection at the edge while capitalizing on advanced data processing in the cloud for further analytics, model updates, and policy fine-tuning. MQTT, a lightweight publish-subscribe messaging protocol, guarantees that even heterogeneous devices communicate openly and rapidly without exceeding the low bandwidth constraints.

4.5 Evaluation Metrics

A comprehensive list of classification and system-level metrics was used to measure the functioning of the system. These included accuracy, precision, recall, and F1 score-and the Receiver Operating Characteristic Area Under Curve (ROC-AUC), which are together used to measure the model's ability to classify between benign and malicious traffic under varying conditions. Additionally, response time was measured from detection to mitigation to represent a real-time response of the system.

Due to the resource constraints of IoT, power profiling tools were used to monitor energy consumption, and system monitors were used to record the memory usage of edge nodes. In this regard, they are important for estimating the feasibility of installing a solution in real-world scenarios where power and memory budgets are very tight. The system was evaluated under different varying loads and attack intensities to test its resilience, scalability, and robustness in a dynamic environment.

5. FINDINGS AND ANALYSIS

The autonomous intrusion detection and response framework powered by AI has been subjected to evaluation in terms of three broad performing dimensions' detection capability, autonomous response efficacy, and deployment viability in resource limited IoT environments. The system has this hybrid detection model (CNN-LSTM with Random Forrest) in place with an aggressive real-time response from a reinforcement learning agent. The evaluations were made on public datasets like UNSW-NB15 and Bot-IoT deployed in a simulated edge-cloud environment.

5.1 Intrusion Detection Performance

Designing the core of the intrusion detection module was done to achieve high detection accuracy resilience against false positives. A comparative evaluation was done between a conventional standalone machine learning model (e.g., a Random Forest classifier with manual feature selection) and the proposed hybrid algorithm integrating deep feature learning and temporal analysis. As summarized in Table 1, it could be seen that the hybrid CNN-LSTM + RF model greatly outperformed the baseline. The hybrid model was able to identify 97.2% of all detections, produce a precision score of 0.94, a recall of 0.96, and an F1-score of 0.95, showing a good trade-off between true positive and false positive rates.

Table 1: Intrusion Detection Performance.

Model	Accuracy (%)	Precision	Recall	F1-Score	False Positive Rate (%)
Standalone ML	90.3	0.88	0.86	0.87	9.20
Hybrid CNN-LSTM + RF	97.2	0.94	0.96	0.95	5.98

The false positive rate (FPR) shown by the hybrid model of 5.98% illustrates a 35% enhancement from the standalone ML baseline. This improvement is vital for IoT deployments, wherein too many false alarms could translate into unnecessary system intervention, resource wastage, and fatigue for management. Furthermore, the integration of CNN and LSTM layers allowed for spatial as well as temporal dependence representation in the data, improving generalization to unseen attack patterns.

5.2 Autonomous Response Mechanism Performance

In addition to detection and classification, this system consisted of a Q-learning-based reinforcement learning agent that autonomously suggested mitigate actions. The objective is for the system to determine the natures of the threats and accordingly choose the best possible response in real time without human intervention. The autonomous agent's performance in various attack scenarios is presented in Table 2. In particular, the agent achieved a hit rate of 91%, which indicates a fairly high accuracy in decision-making. His average response time would be 180 milliseconds, thereby showing compatibility with real time applications.

Table 2: Autonomous Response Mechanism Performance

Metric	Reinforcement Learning Agent
Correct Response Rate (%)	91.0
Average Response Time (ms)	180
False Alarm Rate (%)	4.5

.A false alarm rate of 4.5% indicates that the system has the capability to distinguish between benign anomalies from genuine threats and thus take no excessive or unnecessary action whenever it is triggered. Actions performed by the agent included isolating infected nodes, dynamically rerouting data flows to secure paths, and dispatching administrative alerts. This has a special effect in IoT applications with a very large number of sensors where human intervention becomes impractical for every alert because of scale and latency factors.

5.3 Deployment Feasibility and Resource Efficiency

IoT environments are resource-constrained, wherein edge devices have limited CPU, memory, and power availability. Therefore, an important parameter for determining the feasibility of real-world deployment is the operational footprint assessment of the system. The architecture employed a distributed edge-cloud paradigm whereby lightweight detection was performed at the edge and deeper analyses and coordination were offloaded to the cloud layer. In contrast to that, Table 3 summarizes the average energy consumption and memory usage at both tiers.

Table 3: Deployment Feasibility and Resource Efficiency.

Deployment Layer	Average Energy Consumption (W)	Average Memory Usage (MB)
Edge Node	2.8	130
Cloud Node	7.5	420

For an edge level, this worked on a power envelope of 2.8W, well within the usual limits of typical IoT gateways and smart devices. The memory size of 130 MB was bearable by the cheaper devices. At the cloud level, while power consumption was higher (7.5W and 420 MB), that is acceptable as that resource gets better scaling and computational capacity from the cloud. Therefore, an edge-cloud division of labour ensures that the IDS is both responsive and scalable; both its detection and preliminary mitigation stage is on the edge while it sends the more expensive historical correlation, reinforcement learning updates, and cross-node analytics over to the cloud.

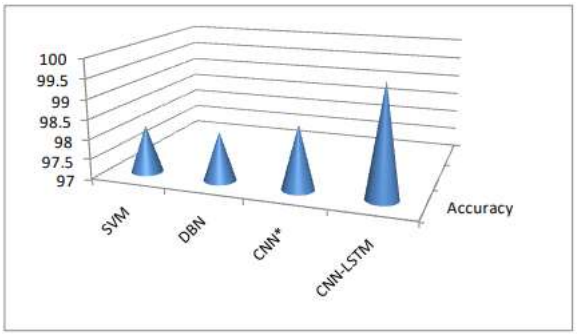

Figure 6: Comparison of Performance Evaluation between Models

6. DISCUSSION

The integration of CNNs and LSTMs with ensemble methods has facilitated much advancement in IDSs in IoT environments. Our study substantiates these findings, showing the hybrid CNN-LSTM model combined with ensemble techniques like Random Forest (RF) can render reliable and accurate detections. Specifically, our model attained a detection accuracy of 97.2% and 0.95 for the F1-score, capitalizing on the shortcoming of the traditional machine learning models. Our results fell in line with earlier research like that of Altunay and Albayrak (2023), who reported that the hybrid CNN-LSTM model achieved 93.21% accuracy for binary classification on the UNSW-NB15 dataset, while another by Sun et al. formed a DL-IDS by CNN-LSTM hybrid network and achieved overall accuracy of 98.67% on the CICIDS2017 dataset. The legions of studies thus point to the successfulness of the hybridization of CNN and LSTM in grabbing spatial and temporal features from network traffic data aimed at enhancing intrusion detection.

Alongside detection, this research has been directed at the realization of an autonomous response mechanism using Q-learning, a reinforcement learning approach. In our case, the Q-learning agent optimally responded in 91% of the tests, with an average response time of 180 ms and a 4.5% false alarm rate. This is in agreement with the work of [54], who developed a Deep Q-Learning (DQL) mechanism for network intrusion detection with promising results in self-learning, outperforming traditional machine learning methods. Thus, reinforcement learning in IDSs would be advantageous as this allows real-time adaptive responses to detected threats without invoking

substantial human interaction; hence making the system more robust overall.

There are still improvements required in adversarial robustness, one of the considered areas. The adversarial attacks on deep learning-based IDS deceive the model into considering malicious activity as benign, through sophisticated inputs [55], assessed the effects of adversarial attacks on deep learning-based IDS and concluded that adversarial attacks could successfully mislead detectors into thinking that malicious activity was normal with a sufficient level of distortion. They pointed out, however, that any possible increase in robustness conferred by adversarial training comes at the price of requiring more data and computational resources. Correspondingly [56], stressed the importance of realistic adversarial robustness analysis and proposed several methodologies aimed at evaluating and improving the resilience of IDS against such attacks. These remarks suggest that although our model shows very high detection accuracy, adversarial training and defence mechanisms against adversarial inputs should form part of our long-term reliability plan. AI-driven IDS must incorporate various other ethical considerations in their deployment, which go from the transparency to the auditability of AI decisions. Stakeholders should understand and trust AI decision-making processes if these AI models were operating in an intelligible manner. This show of transparency is very relevant for security applications. In fact, it is within security where opaque models result in decisions that are unexplainable, often causing harm to the target or otherwise hampering user trust. XAI techniques must therefore be formed into the arena as a tool for mitigating this problem by providing insights into how the models reach a particular decision. In support of explainable AI [57], proposed a hybrid LSTM-Random Forest model for intrusion detection in Wireless Sensor Networks. The logic is that XAI boosts trust in the interpretation of the results produced. The result of integrating XAI methods into IDS will be to produce explanations for their detections and responses that can be understood by the users and enhance their accountability.

Moreover, the presence of resource constraints in the environment has to be considered when deploying an AI-based IDS in any IoT environment. In this regard, our study analysed the resource usage by the system, which shows that edge nodes consumed an average power of 2.8W at the same time consuming 130 MB of memory, while 7.5W and 420MB, respectively, were required by the cloud nodes. Thus, the division of labour enables the IDS to function efficiently within limited computational capabilities of IoT devices. Similar approaches have been adopted in other studies, where hybrid models are designed that balance the computing load between edge and cloud resources so that performance is optimized while the network is not overburdened.

The combination of these models with ensembles is a successful means of improving the robustness of intrusion detection for an IoT environment. Coupled with Q-learning for making autonomous responses, this component significantly strengthens the capability of the entire system to tackle threats in real-time. However, adversarial robustness and ethical issues, as well as transparency and auditability, need to be tackled and incorporated into any trustworthy and resilient AI-based IDS. Future research should centre on strategies such as the incorporation of adversarial training methods, implementation of explainable AI techniques, and improved resource utilization to further increase the effectiveness and efficiency of IDS in IoT networks.

7. CONCLUSION AND FUTURE WORK

This research brings into view the design of a new, autonomous IDS that takes into account the peculiarities and dynamics of IoT environments. The AI techniques of interest feature hybrid ML models in performing temporal pattern recognition and feature extraction, while Random Forest ensemble is used for classification purposes. The proposed system achieves very high detection accuracy and performance robustness for different attack scenarios. A Q-learning-based autonomous response mechanism is incorporated into the proposed solution, allowing for real-time threat mitigation rather than complete dependence on human operators, thereby enhancing system resilience. The findings of the research concluded that combining deep learning with ensemble methods, by far, gives the highest possibility for detection reliability with potential enforcement of proactive and adaptive defence strategies by reinforcement learning. The system, furthermore, maintains suitability for resource-constrained IoT devices following an edge-first architecture model, balancing performance with energy efficiency.

There are still challenges in building adversarial robustness and ensuring ethical transparency. Explainable, auditable, and fair AI-based decisions are paramount to catalyse trust and meet regulatory requirements. Future work will focus on the real-world deployment of the system on IoT testbeds to assess scalability and applicability for these

challenges. Thus, federated learning also would be a good option for distributed model training without centralized data aggregation, preserving privacy and enhancing performance. Finally, leveraging explainable AI (XAI) techniques will be necessary for interpretability and accountability, thereby enhancing the trustworthiness and acceptance of AI-based security systems within IoT networks.

ACKNOWLEDGEMENTS

The author would like to thank Gulf Colleges, Saudi Arabia, for providing support for this research.

REFERENCES

[1] O. Vermesan et al., "Internet of Robotic Things – Converging Sensing/Actuating, Hyperconnectivity, Artificial Intelligence and IoT Platforms," in Cognitive Hyperconnected Digital Transformation, New York: River Publishers, 2022, pp. 97–155. doi: 10.1201/9781003337584-4.

[2] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0," Sensors, vol. 23, no. 16, p. 7194, Aug. 2023, doi: 10.3390/s23167194.

[3] M. Z. Hussain and Z. M. Hanapi, "Efficient Secure Routing Mechanisms for the Low-Powered IoT Network: A Literature Review," Electronics (Basel)., vol. 12, no. 3, p. 482, Jan. 2023, doi: 10.3390/electronics12030482.

[4] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in IoT: a survey," J. Supercomput., vol. 76, no. 7, pp. 5320–5363, Jul. 2020, doi: 10.1007/s11227-019-02945-z.

[5] A. Abdelmaboud et al., "Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions," Electronics (Basel)., vol. 11, no. 4, p. 630, Feb. 2022, doi: 10.3390/electronics11040630.

[6] A. S. George, T. Baskar, and P. B. Srikaanth, "Partners Universal International Innovation Journal (PUIIJ) Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors," 2024, doi: 10.5281/zenodo.10639463.

[7] G. Lindsay, J. C. Brown, B. David Johnson, C. Owens, A. Hall, and B. David, "Microtargeting Unmasked: Safeguarding Law Enforcement, the Microtargeting Unmasked: Safeguarding Law Enforcement, the Military, and the Nation in the Era of Personalized Threats Military, and the Nation in the Era of Personalized Threats Recommended Citation Recommended Citation," Jul. 2023. [Online]. Available: https://digitalcommons.usmalibrary.org/aci_rp

[8] A. Pasdar, N. Koroniotis, M. Keshk, N. Moustafa, and Z. Tari, "Cybersecurity Solutions and Techniques for Internet of Things Integration in Combat Systems," IEEE Transactions on Sustainable Computing, vol. 10, no. 2, pp. 345–365, Mar. 2025, doi: 10.1109/TSUSC.2024.3443256.

[9] A. Tanikonda, B. K. Pandey, S. R. Peddinti, and S. R. Katragadda, "Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems," SSRN Electronic Journal, 2025, doi: 10.2139/ssrn.5102358.

[10] A. Entezari, A. Aslani, R. Zahedi, and Y. Noorollahi, "Artificial intelligence and machine learning in energy systems: A bibliographic perspective," Energy Strategy Reviews, vol. 45, p. 101017, Jan. 2023, doi: 10.1016/j.esr.2022.101017.

[11] M. T. A. Tashfeen, "Intrusion Detection System Using AI and Machine Learning Algorithm," in Cyber Security for Next-Generation Computing Technologies, Boca Raton: CRC Press, 2023, pp. 120–140. doi: 10.1201/9781003404361-7.

[12] P. Panagiotou, N. Mengidis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "Host-based Intrusion Detection Using Signature-based and AI-driven Anomaly Detection Methods," Information & Security: An International Journal, vol. 50, pp. 37–48, 2021, doi: 10.11610/isij.5016.

[13] M. Osaka and B. Scott, "Reinforcement Learning for Autonomous Threat Detection in 5G."

[14] A. Shaddad Abdul-Qawy, P. P. J, E. Magesh, and T. Srinivasulu, "The Internet of Things (IoT): An Overview," 2015. [Online]. Available: www.ijera.com

[15] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.

[16] G. Fortino et al., "Towards Multi-layer Interoperability of Heterogeneous IoT Platforms: The INTER-IoT Approach," 2018, pp. 199–232. doi: 10.1007/978-3-319-61300-0_10.

[17] S. Hamdani and H. Sbeyti, "A Comparative study of COAP and MQTT communication protocols," in 2019 7th International Symposium on Digital Forensics and Security (ISDFS), IEEE, Jun. 2019, pp. 1–5. doi: 10.1109/ISDFS.2019.8757486.

[18] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/j.comnet.2014.11.008.

[19] J. Fan et al., "Understanding Security in Smart City Domains From the ANT-Centric Perspective," IEEE Internet Things J., vol. 10, no. 13, pp. 11199–11223, Jul. 2023, doi: 10.1109/JIOT.2023.3252040.

[20] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: 10.1016/j.comnet.2012.12.018.

[21] M. Adam, M. Hammoudeh, R. Alrawashdeh, and B. Alsulaimy, "A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems," IEEE Access, vol. 12, pp. 57128–57149, 2024, doi: 10.1109/ACCESS.2024.3382709.

[22] J. Kaur Chahal, A. Bhandari, and S. Behal, "Distributed Denial of Service Attacks: A Threat or Challenge," New Review of Information Networking, vol. 24, no. 1, pp. 31–103, Jan. 2019, doi: 10.1080/13614576.2019.1611468.

[23] M. Botnet et al., "Understanding the Mirai Botnet," Aug. 2017.

[24] D. Zheng, Z. Hong, N. Wang, and P. Chen, "An Improved LDA-Based ELM Classification for Intrusion Detection Algorithm in IoT Application," Sensors, vol. 20, no. 6, p. 1706, Mar. 2020, doi: 10.3390/s20061706.

[25] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of Threats to the Internet of Things," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636–1675, Oct. 2019, doi: 10.1109/COMST.2018.2874978.

[26] M. Asadi, M. A. J. Jamali, A. Heidari, and N. J. Navimipour, "Botnets Unveiled: A Comprehensive Survey on Evolving Threats and Defense Strategies," Transactions on Emerging Telecommunications Technologies, vol. 35, no. 11, Nov. 2024, doi: 10.1002/ett.5056.

[27] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man In The Middle Attacks," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027–2051, Jul. 2016, doi: 10.1109/COMST.2016.2548426.

[28] P. M. Rao and B. D. Deebak, "A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions," Ad Hoc Networks, vol. 146, p. 103159, Jul. 2023, doi: 10.1016/j.adhoc.2023.103159.

[29] S. Rani, A. Kataria, and M. Chauhan, "Cyber Security Techniques, Architectures, and Design," in Holistic Approach to Quantum Cryptography in Cyber Security, Boca Raton: CRC Press, 2022, pp. 41–66. doi: 10.1201/9781003296034-3.

[30] I. Martins, J. S. Resende, P. R. Sousa, S. Silva, L. Antunes, and J. Gama, "Host-based IDS: A review and open issues of an anomaly detection system in IoT," Future Generation Computer Systems, vol. 133, pp. 95–113, Aug. 2022, doi: 10.1016/j.future.2022.03.001.

[31] N. Niknami, E. Inkrott, and J. Wu, "Towards Analysis of the Performance of IDSs in Software-Defined Networks," in 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS), IEEE, Oct. 2022, pp. 787–793. doi: 10.1109/MASS56207.2022.00124.

[32] R. Kaur and M. Singh, "A Survey on Zero-Day Polymorphic Worm Detection Techniques," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1520–1549, Mar. 2014, doi: 10.1109/SURV.2014.022714.00160.

[33] G. Bovenzi, G. Aceto, V. Persico, and A. Pescapé, "Blockchain Performance in Industry 4.0: Drivers, use cases, and future directions," J. Ind. Inf. Integr., vol. 36, p. 100513, Dec. 2023, doi: 10.1016/j.jii.2023.100513.

[34] R. K. Pallasena, M. Sharma, and V. Krishnaswamy, "Context-sensitive smart devices - definition and a functional taxonomy," International Journal of Social and Humanistic Computing, vol. 3, no. 2, p. 108, 2019, doi: 10.1504/IJSHC.2019.101593.

[35] M. Jiang, P. Cui, and C. Faloutsos, "Suspicious Behavior Detection: Current Trends and Future Directions," IEEE Intell. Syst., vol. 31, no. 1, pp. 31–39, Jan. 2016, doi: 10.1109/MIS.2016.5.

[36] E. Benkhelifa, T. Welsh, and W. Hamouda, "A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems," IEEE Communications Surveys & Tutorials , vol. 20,

no. 4, pp. 3496–3509, Oct. 2018, doi: 10.1109/COMST.2018.2844742.

[37] A. Heidari and M. A. Jabraeil Jamali, "Internet of Things intrusion detection systems: a comprehensive review and future directions," Cluster Comput., vol. 26, no. 6, pp. 3753–3780, Dec. 2023, doi: 10.1007/s10586-022-03776-z.

[38] O. Alkadi, N. Moustafa, and B. Turnbull, "A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions," IEEE Access, vol. 8, pp. 104893–104917, 2020, doi: 10.1109/ACCESS.2020.2999715.

[39] B. Hameed, A. AlHabshy, and K. ElDahshan, "Distributed Intrusion Detection Systems in Big Data: A Survey," Al-Azhar Bulletin of Science, vol. 32, no. 1, pp. 27–44, Sep. 2021, doi: 10.21608/absb.2021.63810.1100.

[40] Timothy Murkomen, "Performance, privacy, and security issues of TCP/IP at the application layer: A comprehensive survey," GSC Advanced Research and Reviews, vol. 18, no. 3, pp. 234–264, Mar. 2024, doi: 10.30574/gscarr.2024.18.3.0106.

[41] L. Arnaboldi and C. Morisset, "A Review of Intrusion Detection Systems and Their Evaluation in the IoT," May 2021, [Online]. Available: http://arxiv.org/abs/2105.08096

[42] S. K. R. Mallidi and R. R. Ramisetty, "Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: a systematic literature review," Discover Internet of Things, vol. 5, no. 1, p. 8, Jan. 2025, doi: 10.1007/s43926-025-00099-4.

[43] U. Ahmed et al., "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," Sci. Rep., vol. 15, no. 1, p. 1726, Jan. 2025, doi: 10.1038/s41598-025-85866-7.

[44] Y. Guo, "A review of Machine Learning-based zero-day attack detection: Challenges and future directions," Comput. Commun., vol. 198, pp. 175–185, Jan. 2023, doi: 10.1016/j.comcom.2022.11.001.

[45] D. Dwivedi, A. Bhushan, A. Kumar Singh, and Snehlata, "Detection of Malicious Network Traffic Attacks Using Support Vector Machine," In International Conference on Advanced Network Technologies and Intelligent Computing, 2024, pp. 54–68. doi: 10.1007/978-3-031-64064-3_5.

[46] N. Rane, S. P. Choudhary, and J. Rane, "Ensemble deep learning and machine learning: applications, opportunities, challenges, and future directions," Studies in Medical and Health Sciences, vol. 1, no. 2, pp. 18–41, Jul. 2024, doi: 10.48185/smhs.v1i2.1225.

[47] M. Muja and D. G. Lowe, "Scalable Nearest Neighbor Algorithms for High Dimensional Data," IEEE Trans. Pattern Anal. Mach. Intell., vol. 36, no. 11, pp. 2227–2240, Nov. 2014, doi: 10.1109/TPAMI.2014.2321376.

[48] K. M. Abuali, L. Nissirat, and A. Al-Samawi, "Advancing Network Security with AI: SVM-Based Deep Learning for Intrusion Detection," Sensors, vol. 23, no. 21, p. 8959, Nov. 2023, doi: 10.3390/s23218959.

[49] J. Krupski, W. Graniszewski, and M. Iwanowski, "Data Transformation Schemes for CNN-Based Network Traffic Analysis: A Survey," Electronics (Basel)., vol. 10, no. 16, p. 2042, Aug. 2021, doi: 10.3390/electronics10162042.

[50] M. Alshamrani, "IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 8, pp. 4687–4701, Sep. 2022, doi: 10.1016/j.jksuci.2021.06.005.

[51] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," Future Generation Computer Systems, vol. 82, pp. 761–768, May 2018, doi: 10.1016/j.future.2017.08.043.

[52] Y. Meidan et al., "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," IEEE Pervasive Comput., vol. 17, no. 3, pp. 12–22, Jul. 2018, doi: 10.1109/MPRV.2018.03367731.

[53] D. Doshi, T. He, and A. Gromov, "Critical Initialization of Wide and Deep Neural Networks through Partial Jacobians: General Theory and Applications," Oct. 2023, [Online]. Available: http://arxiv.org/abs/2111.12143

[54] H. Alavizadeh, H. Alavizadeh, and J. Jang-Jaccard, "Deep Q-Learning Based Reinforcement Learning Approach for Network Intrusion Detection," Computers, vol. 11, no. 3, p. 41, Mar. 2022, doi: 10.3390/computers11030041.

[55] I. Debicha, B. Cochez, T. Kenaza, T. Debatty, J.-M. Dricot, and W. Mees, "Adv-Bot: Realistic adversarial botnet attacks against network intrusion detection systems," Comput. Secur., vol. 129, p. 103176, Jun. 2023, doi: 10.1016/j.cose.2023.103176.

[56] J. Vitorino, I. Praça, and E. Maia, "SoK: Realistic adversarial attacks and defenses for intelligent network intrusion detection," Comput. Secur., vol. 134, p. 103433, Nov. 2023, doi: 10.1016/j.cose.2023.103433.

[57] R. M. Tolba, Z. T. Fayed, H. A. Alsayadi, N. O. Saad, and T. Elarif, "Detection and Discrimination of Arabic Phonemes Using Long Short-Term Memory (LSTM) Model," in 2023 Eleventh International Conference on Intelligent Computing and Information Systems (ICICIS), IEEE, Nov. 2023, pp. 147–153. doi: 10.1109/ICICIS58388.2023.10391156.