STM JOURNALS

Recent Trends in
Electronics & Communication Systems

ISSN: 2393-8757
Volume 12, Issue 1, 2025
January–April
DOI (Journal): 10.37591/RTECS

https://journals.stmjournals.com/rtecs

Review RTECS

Deep Learning Meets IoT: Hybrid Approaches for Botnet Detection

Sumit Kumar Soni[1,*], Sreeja Nair[2]

Abstract

Rapid advancement in the Internet of Things (IoT) changed everything, making it possible for seamless interconnectivity of devices and altering data-driven decision processes. This study delves into the intersection of IoT with deep learning approaches and hybrid approaches for managing botnet in IoT systems, especially security, efficiency, and performance optimization. Leveraging deep learning models, for example, convolutional neural networks (CNNs) and recurrent neural networks (RNNs), will help the network achieve more intrusion detection and data analysis. Additionally, this paper has further discussed how edge and cloud computing can be used to increase latency, reduce operational costs, and improve data privacy. It also compares different approaches of hybrid security techniques to show how these effectively reduce vulnerabilities in an IoT device. The findings emphasize the potential of integrating deep learning with IoT to develop robust, efficient, and secure systems.

Keywords: IoT, deep learning, edge computing, hybrid techniques, intrusion detection and data privacy

INTRODUCTION

The Internet of Things (IoT) allows for seamless information exchange, monitoring, and control between billions of intelligent machines across various domains, such as home automation, healthcare, agriculture, security, power grids, and critical infrastructure, thereby dynamically digitizing physical systems to bridge the gap between artificial and real environments, or delivering value-added services to mobile and connected devices through purpose-built software equipped to sense, control, and adapt to the state of things [1].

IoT is characterized as a comprehensive, intelligent system that has intelligent data processing, dependable transmission, and comprehensive awareness. By 2025, it is predicted that there will be 75 billion linked "things," up from the current 31 billion. TVs, set-top boxes, entertainment systems, speakers, lights, and heating sensors are among the Smart Home products that private consumers use most [2].

***Author for Correspondence**
Sumit Kumar Soni
E-mail: sonisumit1001@gmail.com

[1]M Tech Scholar, Department of Computer Science, Oriental Institute of Science and Technology, Bhopal, Madhya Pradesh, India
[2]HOD, Department of Computer Science, Oriental Institute of Science and Technology, Bhopal, Madhya Pradesh, India

Received Date: December 02, 2024
Accepted Date: December 08, 2024
Published Date: December 16, 2024

Citation: Sumit Kumar Soni, Sreeja Nair. Deep Learning Meets IoT: Hybrid Approaches for Botnet Detection. Recent Trends in Electronics & Communication Systems. 2025; 12(1): 18–27p.

Television is an example of an IoT display. With a remote control, we can switch the channel stream while we are seated at a distance from the TV without ever touching it. We can remotely operate nearly every electrical appliance in our environment, owing to the same idea behind IoT. Based on how we respond to our behavior in day-to-day life, IoT is a fantastic technology that has an impact on us. Remote-controlled appliances (such as TVs) and electrical home appliances (such as refrigerators and air conditioners) to automobiles offer the quickest and safest path to us. Our smartwatch, and other smartphones, can control anything [3].

The act of linking different physical things, gadgets, and sensors via the Internet so that they can communicate and share data is known as IoT. The healthcare sector is already utilizing IoT technologies to improve patient outcomes and care by opening new channels for remote monitoring, customized treatment plans, and efficient healthcare delivery. The IoT has the potential to fundamentally alter our civilization and is already transforming a number of industries, including healthcare, transportation, and agriculture [4].

Security is one of the most important considerations for a network system to be dependable and effective when conducting transactions over IoT. Owing to the rapid expansion of the IoT across a variety of industries, including manufacturing, education, healthcare, surveillance, and transportation, it is recommended that IoT infrastructure be secured to enhance its functionality [5].

Because data transmitted over the Internet may include industrial secrets, infrastructure information, and safety-critical information, many IoT applications require secure communication. Cryptographic methods such as transport layer security (TLS), which combines symmetric and public key cryptography (PKC), are typically used to accomplish this security. Although these public key cryptosystems are difficult to break with conventional computers, the theoretical underpinnings for resolving their core mathematical issues in polynomial time on a QC were introduced approximately 30 years ago. Despite the lack of strong QCs at the time, cryptography-useful QCs are expected to be available before the end of this decade [6].

Advanced techniques must be developed to provide an acceptable level of security to identify sophisticated cyber-attacks to accomplish the integrated success that guarantees the availability and high performance of advanced communication networks. IoT devices can handle sensitive data, which is a major concern. Owing to their lack of strong security features, many inexpensive commercial products are vulnerable to many types of assault [7].

The limited processing and memory capacities of IoT nodes, complex application-specific infrastructures, and sporadic in-field device upgrades all pose security challenges. Moreover, battery-powered edge devices, which are often utilized in the IoT, sometimes have high energy requirements and a competitively mandated short time-to-market, which often results in serious security risks. As past experiences have shown that security errors can lead to serious financial consequences, a drop in consumer trust, and, in the worst-case scenario, fatalities, this is particularly concerning. IBM found that depending on the industry sector, the average cost of a data breach in 2020 may be as high as $7.13 million. When it comes to “mega breaches,” the price tag can reach $400 million [6].

The special requirements of IoT security can be better met by machine learning systems than by any other method currently in use because they are adaptable, reliable, and scalable. They do not require humans to hard-code patterns; instead, they learn from examples in the available data, self-extract patterns, and create classifiers on new data [8]. Artificial intelligence (AI) has revolutionized all aspects of life by making everything smart, and the IoT has been poised to make life easier by incorporating AI. There is no need for human intervention to improve the quality of life. Weak network protocols and a lack of adequate reliable mathematical analysis techniques plague the IoT, making attacks more frequent [9].

DEEP LEARNING IN IOT

Human specialists are not required for machine learning models to manually set rules regarding dangerous or benign network traffic. They were trained using annotated examples and historical data with class labels for each instance in supervised learning. They then learn to classify the incoming data into various classes by automatically adjusting the parameters of the model. The majority of traditional machine learning algorithms, including Random Forest, Naïve Bayes, Association Rules, Support Vector Machines, k-nearest neighbors, k-means clustering, logistic regression, decision trees, neural

networks, multilayer perceptron (MLP), and Extreme Learning Machines, have been used for IoT intrusion detection system (IDS).

Because of its improved performance, deep learning is rapidly displacing shallow machine learning. Naturally, this trend also extends to IoT intrusion detection. Although deep learning is a subsection of machine learning that includes more intricate models, namely, deep neural networks and several variants, it is recognized as a distinct discipline because of its special qualities [8].

Figure 1 illustrates the data flow in IoT systems, highlighting the roles of IoT devices, edge devices, and cloud computing. This shows how data streaming and fast analysis using deep learning (DL) methods occur at edge devices, whereas IoT clouds handle large-scale data analysis using advanced DL techniques.

In a variety of IoT applications, DL is better able to generalize the dynamic interaction of vast amounts of raw data than typical machine learning algorithms. Common learning models can be easily overtouched when dealing with a deluge of data, whereas DL models are likely to perform better with big data. This is because the processing capacity usually depends on the depth and various learning model architectures such as convolutional architectures. DL can extract successful features from raw data without the need for laborious manual applications.

In recent years, DL models have been more thoughtful than other traditional ML techniques. Figure 2 displays the Google Trends search pattern, where DL is becoming increasingly well-liked among other machine learning algorithms such as decision trees, random forests, k-means, and SVM. Furthermore, Figure 3 indicates that the Convolutional Neural Networks (CNNs) approach has gained popularity among all DL methods, in accordance with Google Trends [10].

There are several hidden layers, an output layer, and an input layer in the DL architecture used to monitor cutting stability. To identify the machining status, DL uses several hidden layers to process the force-signal input data.

The network is composed of interconnected artificial neurons in each layer. The artificial neuron in the layer l_i computes its output by passing the input from the weighted prior output of the layer l_{i-1} through a nonlinear activation function. The nodes of the final layer, which represent the model's targets, will then receive this result and pass it on to the following layer, l_{i+1}.

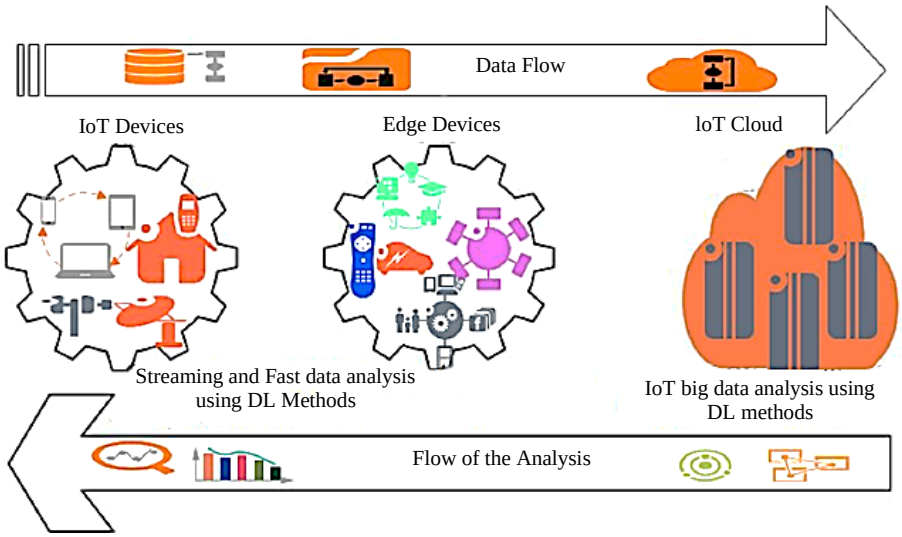

Figure 1. Data generation and processing of IoT [11].

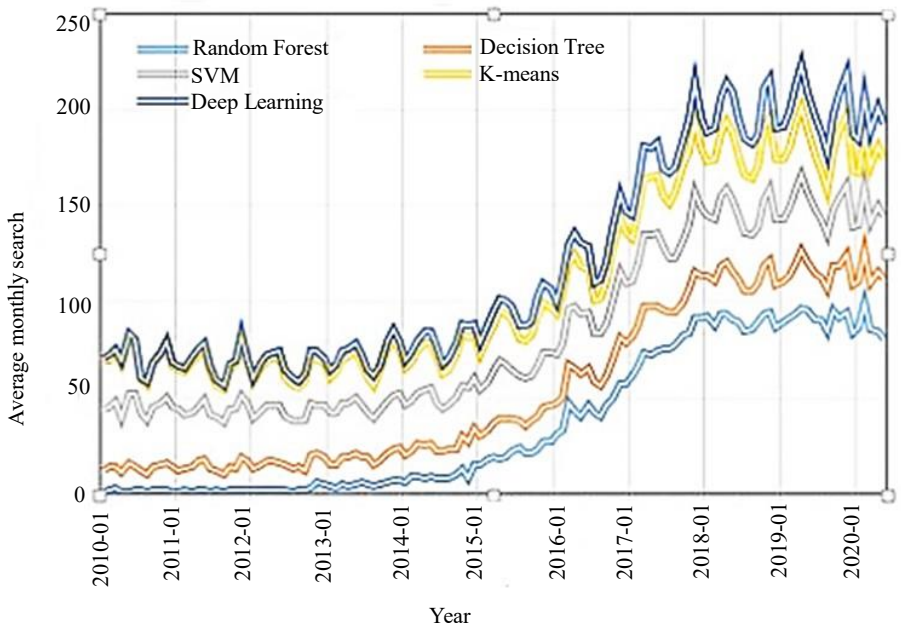

Figure 2. Recent years have shown an increase in interest in DL, according to Google Trends [10].

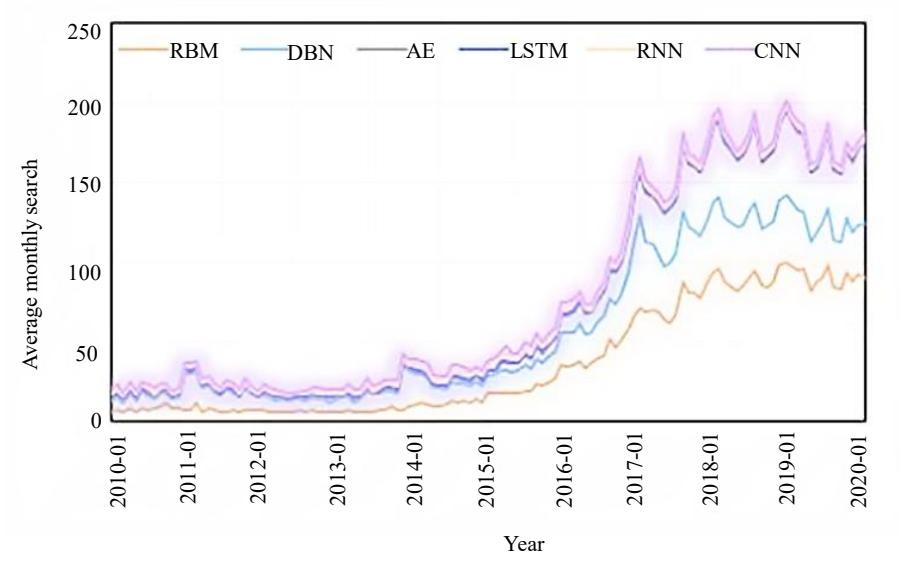

Figure 3. Google Trends indicates increased attention to CNN in the past few years [10].

Therefore, if the processing capacity is sufficient, the network can learn extremely complex functions. Eq. (1) describes the deep neural network's nonlinear interaction between two neighboring layers. This illustrates how the (l − 1) th layer changes into neuron j in the lth layer, where the hidden representations of the (l − 1) th and the i^{th} layers are represented by the letters l and l−1, respectively.

$$a_j^I = \sigma(\sum_k w_{jk}^I a_k^{I-1} + b_j^I) \tag{1}$$

The weight matrix connecting node k in layer (l-1) to node j in layer l to the ith layer of neurons is denoted by w_{jk}^i. Additionally, the bias vector for each layer l is b_j^i additionally, the rectified linear unit (ReLU), which is established in Equation (2), was utilized in this study as the activation function, where σ represents the activation function.

$$\sigma(x) = \max(o, x), \tag{2}$$

To determine the probability for each potential class, we employed the SoftMax function as an activation function in the output layer. Equation (3) formulates the SoftMax function:

$$y_c = \frac{\exp(a_c)}{\sum_{i=1}^{k} exp(a_i)} \tag{3}$$

where a_c is the value of the input vector to the SoftMax function, and the term of $\sum_{i=1}^{k} \exp(a_i)$ is the normalization term that makes the summation of all the output values of the function equal to 1. K = 3 represents the number of classes. Therefore, the predicted label is determined using the largest output value [11].

A new IDS was described by HAST-IDS, a hierarchical spatial-temporal feature-based IDS. Long Short-Term Memory (LSTM) is used to learn temporal features at high levels after HAST-IDS represents spatial features via network traffic at low levels, which are learned using deep CNNs. IDS has employed a variety of DL techniques, and three models: a "vanilla deep neural net" (DNN), a "self-taught learning" (STL) method, and a Recurrent Neural Networks (RNN)-based LSTM-are assessed for accuracy and precision. The young network was designed to identify threats using a bidirectional LSTM RNN (BLSTM RNN), according to a novel DL system.

The design of "Particle Swarm Optimization" (PSO) utilizing learning factors and adaptive inertia weight is part of the Deep Belief Networks (DBN) network structure that has been optimized by suggesting a new structure. PSO is then created by utilizing the behavior of the fish swarms. With the use of the DL approach, which combined the "Random Forest" (RF) Algorithm with DT Classifiers, the suggested system was able to detect attacks more accurately and eliminate irrelevant characteristics [10]. The DL classification used for assault detection is shown in Figure 4.

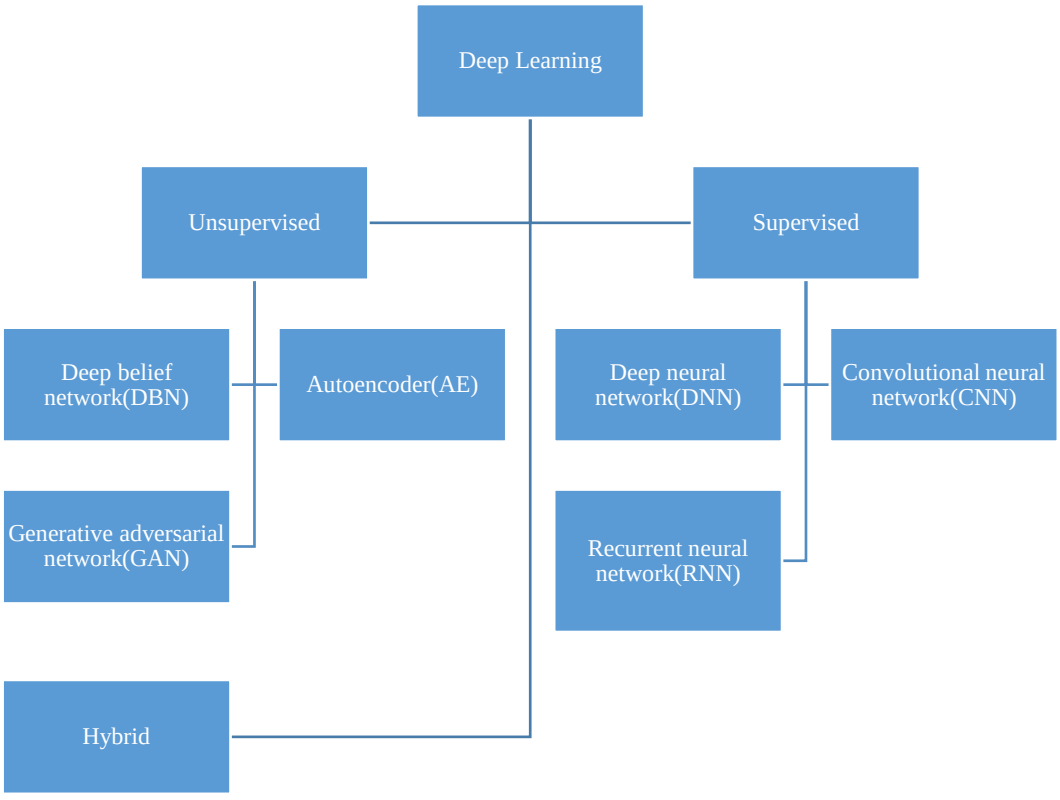

Figure 4. General classification of DL [9].

COMPARATIVE ANALYSIS OF HYBRID TECHNIQUES

Hybrid approaches are emerging that combine multiple solutions to address the shortcomings of earlier approaches. We can obtain good outcomes from this combination, as we will see in the following works. Distributed method for Wireless Sensor Network (WSN) outlier detection based on k-nearest neighbors (KNN) and fixed-width clustering algorithms. They clustered the data values locally at each node, balancing the load and lowering the communication overhead. The parent node then receives the cluster summary from each node to combine the related clusters according to the cluster width. This process is repeated until they arrive at the main station, which uses the KNN parameters to calculate the inter-cluster distance and identify the outliers. The performance of the distributed algorithm is superior to that of the centralized algorithm [12].

FlyNetSim is an integrated unmanned aerial vehicle (UAV)-Network Simulator that uses the Python programming language to implement the suggested hybrid approach for enhancing the security of UAVs for IoT applications. Numerous dispersed sensors were constructed over the simulator, and the blockchain system was intended to serve as a test bed for a deployment scenario utilizing a variety of machine learning algorithms. Using an API and a Python scikit module, KNN, Naïve Bayes (NB), and multiclass classifier Onevsrest are integrated into a blockchain scenario.

To provide security and privacy in multiple header blockchain architectures, hash functions offer security encryption with blocks. The transactions incorporate several ML techniques that have been described. Block-chain-enabled UAVs offer asymmetric encryption methods and authentication and authorization processes, which contribute to the protection of data privacy in drone network security [13].

Table 1 provides an overview of various IoT devices, their associated attack types, vulnerabilities, and implemented security measures. It mentions common challenges such as buffer overflows, unencrypted communication channels, unsecured APIs, and weak password protection. Further proposed measures range from cryptographic techniques and API endpoint security to multi-factor authentication and access restrictions. This analysis stresses the need for advanced and hybrid security approaches that may integrate lightweight encryption and machine learning techniques to effectively counter the evolving vulnerabilities of IoT.

Table 1. Comparative analysis of security measures in IoT devices.

IoT Device	Attack Type	Device Vulnerabilities	Measures
Smart Vehicle	Device software failure	Buffer overflows	Address space layout randomization (ASLR) and stack guard, dynamic verification techniques
Smart Industrial Devices	Node tampering attack	Hardware replacement	Tamper-resistant cryptography techniques, elliptic curve integrated encryption scheme (ECIES)
Smartphones, Measuring Devices	Eavesdropping attack	Unencrypted communication channels	Lightweight cryptography encryption techniques, attribute-based encryption, proxy re-encryption
Smart Thermostat, Smart Bulb	Malicious code injection	Unsecured APIs and lack of integrity checks	API endpoint security, delete-setting, and configuration
Smart Car, Smart TV	Unauthorized access	Device and application vulnerabilities	Regular updates and secure key generation
Smart Healthcare, Smart Speakers, Garage Door Openers	Social engineering attack	Weak password protection	Multi-factor authentication, collision-resistant one-way hash function
Drone, IoT Gas Pump	Device hardware exploitation	Open insecure hardware interface	Access restrictions
IP Camera, Smart Home Devices	Malicious node insertion	Weak encryption schemes	Symmetric key encryption, signing mechanisms

The most widely utilized self-learning algorithms for malware detection are CNN and RNN. Natural language processing (NLP) is effective in spotting social engineering and spam assaults by using novel language patterns and communication channels. Artificial Neural Networks (ANN) are highly effective in tracking network activity and identifying potential threats. A feed-forward neural network can be used for supervised instance learning, such as CNN, DNN, and ANN. Both the RNN and LSTM fall within the category of supervised sequence-learning techniques.

Semi-supervised instance learning is used by DBN and Restricted Boltzmann Machines (RBM). To create generic issue statements and reuse them with other models, DL also enables transfer-learning techniques. While AE, DBN, RBM, and generative adversarial network (GAN) are generative DL approaches, CNN and RNN are the most widely used techniques for conditional/discriminate models; their combination is referred to as an ensemble methodology [14].

The Role of Edge and Cloud Computing in IoT Security

Cloud

Cloud computing is considered a special way to provide business applications [10]. It provides services, particularly via the Internet, using various hardware and software components. Initially, cloud computing made it easy to access a variety of data and applications. A number of industry titans and standards organizations have made efforts to define cloud computing in their terms [15].

One of the main advantages of cloud computing is its capacity to provide organizations and consumers with access to remote computing resources, enabling them to take advantage of strong computational skills without requiring a significant amount of local equipment. These resources are often hosted and managed by centralized data centers in cloud computing infrastructure, which provides customers with cost-effectiveness, scalability, and flexibility. Users can access apps, save data, and perform computational operations without being restricted to particular physical places because of cloud computing, which distributes cloud services via the Internet [16].

It is possible to deploy private, public, hybrid, and community cloud types as shown in Figure 5. Many Internet users can access the services offered by public clouds. Private enterprises can access specific services through private cloud services. The goal of a community cloud is to offer services to a collection of businesses. Finally, hybrid clouds allow businesses to strike a compromise between cost and control difficulties [17].

Figure 5 depicts three main cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS provides software applications to users such as Google Apps and Hotmail. PaaS provides a platform for application development along with tools such as the Google App Engine and Microsoft Azure. IaaS delivers virtualized computing resources; Google Compute Engine and Amazon EC2 allow businesses to manage their infrastructure requirements.

Global investment in cloud service infrastructure is expected to reach $1 trillion by 2024, driven by a number of current trends such as increased demand for cutting-edge platforms and as-a-service solutions, particularly those that incorporate AI. Businesses now see the cloud as a strategic enabler for fostering innovation, improving agility, and attaining success in a variety of industries rather than just as a way to save costs. The rise in cloud costs and the growing use of cutting-edge AI technologies, such as ChatGPT, influence the direction of cloud computing trends. To increase productivity and improve client interactions, businesses are rapidly moving their operations to cloud-based systems. Additionally, businesses will continue to use cloud services to gain access to advanced technology, which will increase the overall effectiveness of their processes [18].

Edge

To distribute resources at the network edge or closer to various home and office appliances such as clients, IoT devices, mobile devices, and client sensors, Edge, a revolutionary computational offloading method, was created.

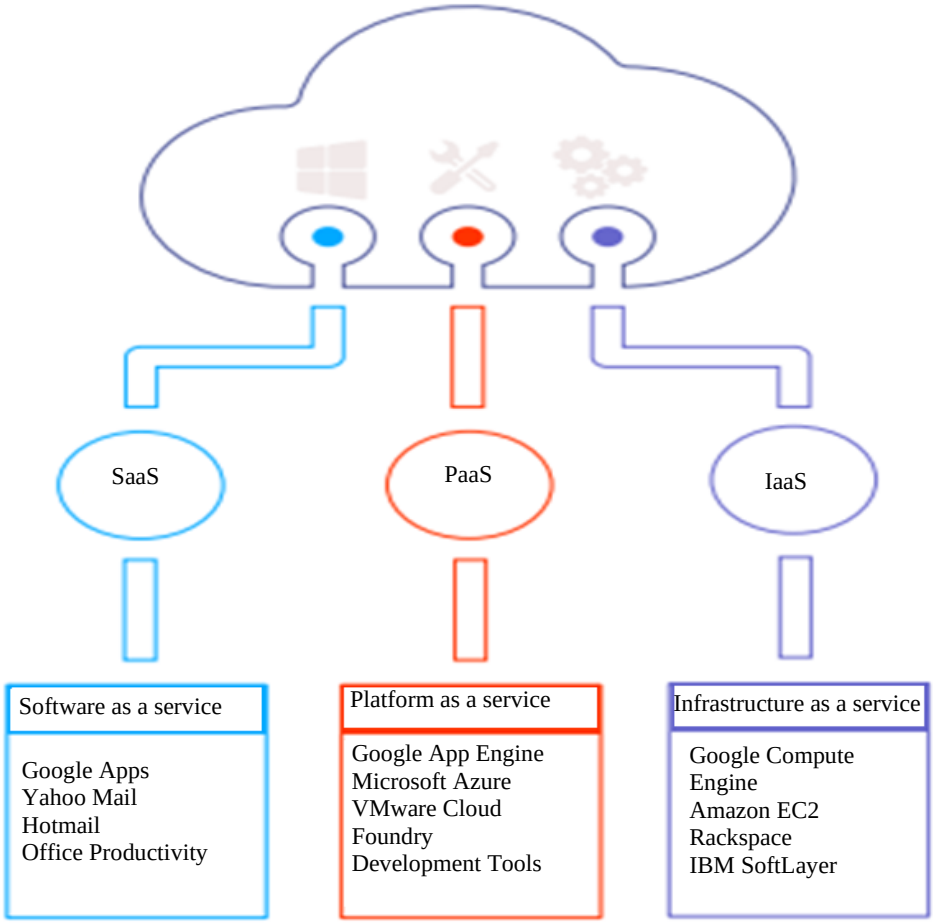

Figure 5. Cloud computing services [17].

Recently, there has been a sharp increase in research and industrial investments in edge computing. Physical closeness and accessibility are crucial to edge computing because they affect end-to-end latency. This essential feature of cloudlets guarantees their existence, encourages confidence, and lowers the cost of bandwidth [15]. Additionally, edge computing is closely related to other concepts, such as fog computing, mobile edge computing (MEC), and mobile cloud computing (MCC), each of which has unique architectural features and focus areas [17].

Edge computing offers several advantages. By enabling millisecond-level data processing, reducing delays, and requiring less connection bandwidth, the system performance is enhanced. By decreasing data transfer and cloud storage, enabling the local deployment of security measures, and lowering the danger of data leakage, it improves data security and privacy. Being close to users lowers latency; however, performance may occasionally be impacted by local computation constraints. As edge computing lowers bandwidth consumption, data transmission volume, and related costs, the operational costs decrease.

Because it uses small data centers and hybrid models for more processing capabilities, it does not meet the requirements for centralized platforms, increasing service availability. Finally, edge computing is resilient to connectivity problems, minimizing reliance on pricey connectivity solutions and enabling continuous application operations in places with inadequate network coverage [19].

CONCLUSION

This study points out the transcendent benefits that result from the integration of DL with IoT to overcome critical challenges, including vulnerabilities, botnets for data processing, and system

inefficiencies. Using advanced DL models, IoT systems can achieve significant improvements in intrusion detection accuracy and real-time data analysis. A comparative analysis of hybrid techniques reveals their effectiveness in addressing diverse security threats of IoT, ranging from unauthorized access to hardware exploitation.

Moreover, edge and cloud computing technologies provide augmented system performance while decreasing latency. Robustness in service availability was ensured. The insights from this study will provide a comprehensive foundation for the development of innovative and secure IoT applications for smarter and safer digital ecosystems.

REFERENCES

1. Mohammed Sadeeq M, Abdulkareem NM, Zeebaree SRM, Mikaeel Ahmed D, Saifullah Sami A, Zebari RR. IoT and cloud computing issues, challenges and opportunities: A review. Qubahan Academic Journal. 2021;1:1–7. DOI: 10.48161/qaj.v1n2a36.
2. Schiller E, Aidoo A, Fuhrer J, Stahl J, Ziörjen M, Stiller B. Landscape of IoT security. Computer Science Review. 2022;44:100467. DOI: 10.1016/j.cosrev.2022.100467.
3. Laghari AA, Wu K, Laghari RA, Ali M, Khan AA. A review and state of art of Internet of Things (IoT). Arch Comput Methods Eng. 2021;1–19.
4. Li C, Wang J, Wang S, Zhang Y. A review of IoT applications in healthcare. Neurocomputing. 2024;565:127017.
5. Sattari F, Farooqi AH, Qadir Z, Raza B, Nazari H, Almutiry M. A hybrid deep learning approach for bottleneck detection in IoT. IEEE Access. 2022;10:77039–53. DOI: 10.1109/ACCESS.2022. 3188635.
6. Schöffel M, Lauer F, Rheinländer CC, Wehn N. Secure IoT in the era of quantum computers: Where are the bottlenecks? Sensors. 2022;22:2484. DOI: 10.3390/s22072484. PubMed: 35408099.
7. Alashhab A, Zahid MS, Muneer A, et al. Low-rate DDoS attack detection using deep learning for SDN-enabled IoT networks. [Preprint]. TechRxiv. 2024 Jan 8. doi: 10.36227/techrxiv.170472893. 31491821/v1.
8. Tsimenidis S, Lagkas T, Rantos K. Deep learning in IoT intrusion detection. J Netw Syst Manag. 2022;30:8. doi: 10.1007/s10922-021-09621-9.
9. Jasim AD. A survey of intrusion detection using deep learning in internet of things. Iraqi J Comput Sci Math. 2022;3:83–93.
10. Lakshmanna K, Kaluri R, Gundluru N, Alzamil ZS, Rajput DS, Khan AA, et al. A review on deep learning techniques for IoT data. Electronics. 2022;11:1604.
11. Tran MQ, Elsisi M, Liu MK, Vu VQ, Mahmoud K, Darwish MMF, et al. Reliable deep learning and IoT-based monitoring system for secure computer numerical control machines against cyber-attacks with experimental verification. IEEE Access. 2022;10:23186–97. DOI: 10.1109/ACCESS. 2022.3153471.
12. Samara MA, Bennis I, Abouaissa A, Lorenz P. A survey of outlier detection techniques in IoT: Review and classification. J Sens Actuator Netw. 2022;11:4. DOI: 10.3390/jsan11010004.
13. Abualsauod EH. A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network. Comput Electr Eng. 2022;99:107847. DOI: 10.1016/j. compeleceng.2022.107847.
14. Jayalaxmi PLS, Saha R, Kumar G, Conti M, Kim TH. Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey. IEEE Access. 2022;10:121173–92. DOI: 10.1109/ACCESS.2022.3220622.
15. Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. Sensors. 2022;22:927. DOI: 10.3390/s22030927. PubMed: 35161675.
16. Rupanetti D, Kaabouch N. Combining edge computing-assisted Internet of things security with artificial intelligence: Applications, challenges, and opportunities. Appl Sci. 2024;14:7104. DOI: 10.3390/app14167104.

17. Laroui M, Nour B, Moungla H, Cherif MA, Afifi H, Guizani M. Edge and fog computing for IoT: A survey on current research activities & future directions. Comput Commun. 2021;180:210–31. DOI: 10.1016/j.comcom.2021.09.003.
18. Rehan H. Revolutionizing America's cloud computing the pivotal role of AI in driving innovation and security. J Artif Intell Gen Sci. 2024;2:239–40. DOI: 10.60087/jaigs.v2i1.110.
19. Fazeldehkordi E, Grønli TM. A survey of security architectures for edge computing-based IoT. IoT. 2022;3:332–65. DOI: 10.3390/iot3030019.

