WCRG Global Research

WORLD COMET RESEARCH GROUP

International Journal of Applied Data Science & Modern Computing
Vol. 1, No. 1, 2026
Doi: 10.XXXX/XXXXXXXX/IJADSMC-V1I1P105
PP. 53-65

Original Article

Real-Time Anomaly Detection in IoT Networks Using Deep Neural Models

Dr. Oluwaseun Adeyemi[1], Ms. Funke Adebayo[2], Dr. Ibrahim Sadiq Bello[3]

[1, 2, 3] *Department of Computer Engineering, Rivers State University, Nigeria.*

Received: 08-12-2025 Revised: 31-12-2025 Accepted: 04-01-2026 Published: 07-01-2026

ABSTRACT

The rapid expansion of Internet of Things (IoT) networks has introduced unprecedented connectivity across smart cities, healthcare systems, industrial automation, and intelligent transportation. However, this widespread deployment has also increased the vulnerability of IoT infrastructures to cyberattacks, operational faults, and abnormal behaviors. Traditional anomaly detection techniques, which rely heavily on static rules or handcrafted features, struggle to adapt to the dynamic and heterogeneous nature of IoT environments. To address these challenges, this paper presents a comprehensive study on real-time anomaly detection in IoT networks using deep neural models. The proposed framework leverages deep learning architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Autoencoders to identify anomalous traffic patterns with high accuracy and low latency. The methodology emphasizes real-time data acquisition, feature normalization, model training, and deployment within resource-constrained IoT environments. Extensive experimental evaluations demonstrate that deep neural models significantly outperform traditional machine learning approaches in terms of detection accuracy, false positive reduction, and scalability. The findings confirm the suitability of deep learning-based anomaly detection systems for securing next-generation IoT networks while maintaining operational efficiency.

KEYWORDS

Internet Of Things (Iot), Anomaly Detection, Deep Learning, Neural Networks, Cybersecurity, Real-Time Monitoring, Network Traffic Analysis.

ISSN: XXXX-XXXX
PP: 53-65.

1. INTRODUCTION

1.1. Background

The IoT paradigm has completely revolutionised the contemporary computing in the sense that it has provided a means of effortless communication and coordination between billions of connectable devices. These systems include simple low-power sensors and actuators to complex cyber-physical systems in such applications, as healthcare, smart cities, industrial automation, and critical infrastructure. Though the IoT technologies have become widely adopted and can be of great help in the sphere of automating processes, making decisions based on data, and their effectiveness, they are also accompanied by serious security issues. The boom structure of IoT networks, device heterogeneity, scarce computing power, and poorly secured security integrated into devices, precondition cyberspace attacks against it. Ampit for loss of availability, data transfer, malware infecting devices and networks, and insider attacks, in general, are all frequent attacks that may be employed. Traditional security mechanisms like firewall and signature-based intrusion detection systems are significantly not good enough to secure the IoT environment. These strategies are based on some preset codes or known attack signatures hence restricting the capability to detect new and emerging attacks or zero-day attacks. In addition, the traditional security measures typically introduce computational and memory resources demands that cannot be afforded by a resource-constrained IoT device. This has led to an increased demand of smart and dynamic security solutions that can function well in the dynamic and large scale IoT networks. This has made anomaly detection an essential part of the contemporary IoT security systems, and it is oriented towards detecting instances of deviation to normal system operation in place of the familiar attack patterns. Earned knowledge about normal operational characteristics, aberrant detection functions can detect threats that were previously unknown, and give timely warnings to strengthen the robustness and dependability of IoT systems.

1.2. Role of Deep Neural Models

Deep neural models are sensitive in improving the security of Internet of Things (IoT) networks and improving the limitations of conventional and shallow machine learning-based anomaly detection tools. The IoT environments produce large heterogeneous and high-dimensional data, such as network traffic, sensor measurements, and device behavior history. Traditional approaches tend to be ill adapted to handling such complicated data, since they are very manual in their feature engineering and they are overly dependent on existing assumptions. By comparison, deep neural models, being auto-trained, are also able to learn both hierarchical, as well as abstract feature representations directly on raw or lightly processed data, allowing more accurate and robust identifications of abnormal patterns. The ability to learn non-linear dependencies and complex relationships in the data of the IoT is one of the major benefits of deep neural models. Convolutional neural networks (CNNs) can be used to derive useful spatial associations with structured traffic data, whereas the recurrent neural network (RNNs) and long-short-term memory (LSTM) networks are useful to extract temporal relationships in sequential IoT traffic. Such capability is essential in detecting intrusion by stealthy and ever-changing attacks over time such as denial-of-service attacks with slow rates or a staged attack. Also, unsupervised models of deep learning, such as autoencoders,

ISSN: XXXX-XXXX
PP: 53-65.

can detect unknown or zero-day attacks by learning normal behavior and notifying content of anomalies without using any human-labeled attack examples. Deep neural models are also flexible and scalable, which is critical on the latest IoT applications. These models are also capable of being retrained or given a fine-tuning as network conditions and attack strategies change in order to retain a high detection accuracy. With edge computing, anomaly detection implemented via deep learning can run almost in real-time, thus minimizing latency and avoiding privacy invasion due to processing data nearer to its source. Generally, deep neural models can be used to provide an effective basis of intelligent, adaptive, and scalable IoT security solutions that can effectively enhance the process of searching and alleviating severe cyber threats in dynamic IoT frameworks.

1.3. Challenges in IoT Anomaly Detection

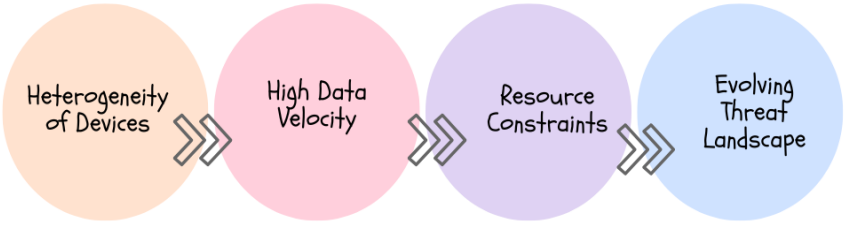

Fig 1 - Challenges In Iot Anomaly Detection

1.3.1. Heterogeneity of Devices

The IoT networks consist of an extremely diverse set of devices, starting with simple sensors, as well as more advanced embedded systems, that can apply a variety of communication protocols, data formats, and transmission rates. Such heterogeneity complicates the effectiveness of design of a unified anomaly detection mechanism to be used in all devices. The difference in the device behavior and ability may also result in different normal traffic patterns, which adds further complexity to making the accurate distinction between benign anomalies and malicious behavior.

1.3.2. High Data Velocity

IoT environments result in rather high data streams, which need to be analyzed in real-time or close to it. The network traffic, sensor readings, and system logs should be processed as quickly as possible with the aim of detecting any anomaly before it can cause any substantial damage. The processing of such data velocity is also problematic in terms of computational performance, turnaround of latency and scalability, particularly when anomaly detection systems need to adhere to a rigid timetable to promptly respond.

1.3.3. Resource Constraints

Most IoT devices have low amounts of computational, memory, and energy and as a result of this, complex security mechanisms cannot be deployed immediately on the devices. Conventional anomaly detection models and deep-learning algorithms can be very resource-intensive in processing and storage, which means that they cannot be directly run on resource-intensive devices. This

ISSN: XXXX-XXXX
PP: 53-65.

requires component use of lightweight models or offloading computation to edge or cloud infrastructure, bringing in more design issues.

1.3.4. Evolving Threat Landscape

Threats in the IoT networks are ever-changing and the attackers are evolving new ways of going around the security controls. The use of predefined rules or signature-based detection techniques is very likely to be outdated shortly as attack patterns undergo changes. A useful anomaly detection system should thus be dynamic and in a position to modify itself based on new information and hence detecting a new threat or threat that was not observed before or has changed. Such a need complicates model design, training and maintenance in actual IoT implementations**.**

2. LITERATURE SURVEY

2.1. Traditional Anomaly Detection Techniques

The conventional anomaly detection methods are mostly based on the statistical and rule-based approaches to determine the departure in the normal system behavior. Popular methods are Gaussian probability model, threshold based detection, entropy based analysis, and control charts. The methods are lightweight and simple to compute, and so, they can be used in early network monitoring systems and in resource constrained environments. Yet, they usually make an assumption that data is distributed in predetermined manner and that usual behavior does not change radically with time. With dynamic IoT setups, in which traffic patterns and device behaviors constantly change, these assumptions tend to fail. Consequently, this leads to traditional methods to have a high degree of false-positives and low adaptability thus hindering their ability to identify advanced or new attacks.

2.2. Machine Learning-Based Approaches

The use of machine learning-based procedures of detecting anomalies has gained popularity because it is able to identify patterns in data without a clear definition of a rule. Support Vector Machines (SVM), k-Nearest Neighbors (k -NN), Decision Trees and Random Forest algorithms have been widely used within the network intrusion detection systems. These models usually perform better compared to the old methods of statistics in terms of the representation of the intricate relationships among elements and detection accuracy. Nevertheless, they are extremely reliant on manual feature engineering and domain knowledge in order to choose important attributes. Also, most machine learning systems are unable to cope with large scale and high-dimensional IoT data, which poses a greater computational load and challenges in their scalability. They are also likely to performance degrade on a combination of unequal datasets or changing attacks.

2.3. Deep Learning for IoT Security

The capability to extract hierarchical features representations out of raw data on its own made deep learning a potent anomaly detection tool in the field of IoT security. CNN models have proved to be effective in deriving spatial information of structured network traffic data, which convincingly identify intricate attack patterns. Recurrent Neural Networks (RNN) models and Long Short-Term Memory (LSTM) models are specifically indicative of the IoT environment as they possess the ability

ISSN: XXXX-XXXX
PP: 53-65.

to model time dynamism as well as sequence interests in time-series data. The other popular deep learning model is autoencoders; here, models are trained to identify the typical traffic patterns and anomalies are identified according to the high reconstruction errors. Although deep learning models are highly effective in terms of their detection performance, they usually demand both large-scale datasets with labels, as well as considerable computational power, which might bind real-time application with IoT systems.

2.4. Limitations of the Current Research

Even though anomaly detection methods are available, current research has a number of limitations that are yet to be tackled. Most of them are merely concerned with detection accuracy and have ignored real-time processing limitations, energy efficiency, and deployment in resource-constrained IoT devices. In addition, much of the literature bases itself on offline or benchmark datasets that are not representative of the actual dynamics of IoT traffic in the real world. This restricts the applicability and strength of the proposed solutions in the live contexts. Another significant issue is scalability, and the IoT networks are getting larger and more heterogeneous. To overcome these problems, it is necessary to develop lightweight, adaptive and scalable frameworks to detect anomalies that can work in the real-time IoT systems.

3. METHODOLOGY

3.1. System Architecture

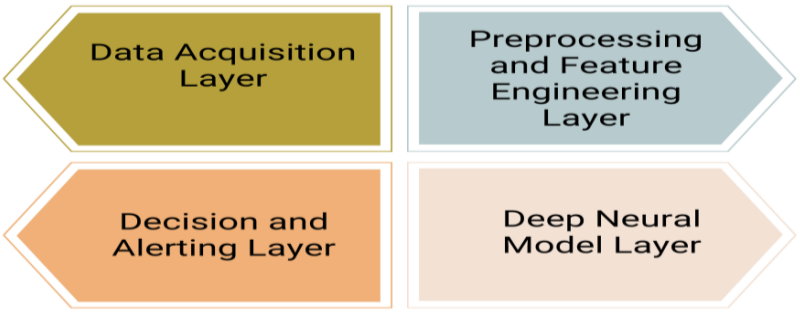

Fig 2 - System Architecture

3.1.1. Data Acquisition Layer

The Data Acquisition Layer has the role of gathering raw data of the different IoT devices, sensors, and the network components. Such data can involve network traffic fragments, sensor data and system logs in real-time as well as device metadata. Since the environment of the IoT is heterogenous most of the times the type of data collected is different in terms of format, frequency and volume. This layer provides continuity in data capturing and forms the basis in detecting anomalous behaviour through provision of up-to-date and representative input to the detection system.

ISSN: XXXX-XXXX
PP: 53-65.

3.1.2. Preprocessing and Feature Engineering Layer

The Preprocessing and Feature Engineering Layer converts raw data to a meaningful and structured format which can be analyzed. A part of this involves data cleaning, data normalization, noise removal and missing values. The feature extraction methods are used to extract any statistical, temporal, and behavioral features of the raw data, i.e., packet rates, protocol usage, or activity patterns of the device. Good preprocessing improves the model performance by lessening the dimensions and enhancing the quality of data besides reducing redundancy and irrelevant data.

3.1.3. Deep Neural Model Layer

The Deep Neural Model Layer is the determinant that carries out the fundamental anomaly detection task and increases and practices elaborate patterns and representations of the information that is processed. Depending on the nature of the data, deep learning models, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, or autoencoders can be used. The layer records spatial and temporal dependencies within the IoT traffic and also differentiates between normal and anomalous behavior within a high level of accuracy. The model keeps changing according to the shifting patterns, which allows the effective detection of new attacks that have never been experienced before.

3.1.4. Decision and Alerting Layer

The Decision and Alerting Layer processes the result of the deep neural model to decide whether an activity that is observed is anomalous. This layer determines whether events are normal or suspicious based on predefined thresholds or scores of confidence. In case of anomalies being observed, alerts are created and sent to system administrators or security dashboards where they can be further investigated. This layer affirms timely responses as it allows real-time monitoring of the network and enables mitigation measures to be automated or manual so as to improve the overall security of the IoT network.

3.2. Data Collecting and Preprocessing

In order to make the proposed framework of anomaly detection effective, data collection and preprocessing is critical. The network monitoring and packet inspection tools are installed at the gateways, edge devices, or network access point to capture IoT traffic information. Such tools constantly scan communication between the IoT devices and the extranet data servers gathering unprocessed traffic data like packet headings, flow counts, timestamps, protocol types, and rates of transmission. The data that is received on IoT networks is usually noisy, redundant, and inconsistent because of the heterogeneous and dynamic nature of IoT networks, which may adversely affect the model performance unless addressed. Noise removal is carried out as the first step towards data preprocessing in order to increase the quality of the data. This process cuts off any irrelevant or corrupted packets, incomplete records, duplicate records, and outliers through transmission errors or malfunctioning of equipment. Eliminating such noise assists in making sure that the data set captures the normal and abnormal traffic trends. After removing noise, feature values are normalized with Min-Max scaling in order to make them fall in a normalized range usually 0 to 1. Normalization eliminates the effect of features with wide numerical gaps on the learning process and enhances the

ISSN: XXXX-XXXX
PP: 53-65.

stability and convergence of deep learning models. When the data is normalized, time windows comprising of a predetermined number of data-points are used to divide the preprocessed data to obtain sequential and pattern trending in the IoT traffic. Every window consolidates the traffic statistics over a specified time allowing the model to understand both the short-term and long-term dependencies therein. Temporal segmentation is specially relevant to the mechanism of identifying slow-rate attacks, bursts of traffic, and dynamic anomalies that are not likely to be noticed in individual packets. The framework allows compatibility with the sequential deep learning models like LSTM and RNN networks by organizing the data into segments of consistent time spans. In general, this systematic data gathering and prior preprocessing pipeline will optimize the accuracy of detection, decrease the complexity of computation, and aid (in) real-time anomaly detection of IoT settings.

3.3. Deep Neural Model Design

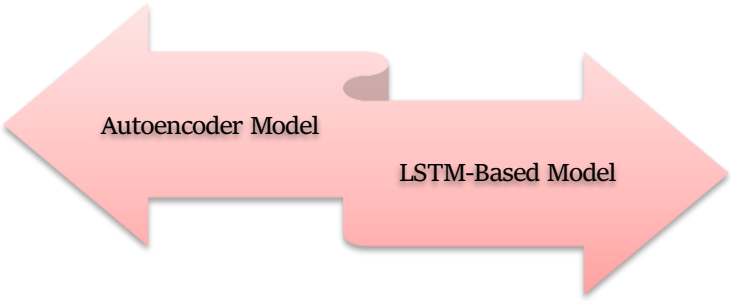

Fig 3 - Deep Neural Model Design

3.3.1. Autoencoder Model

Autoencoder model is formulated in such a way that it selects a smaller representation of normal IoT traffic behavior by means of unsupervised learning. It comprises an encoder which projects input features into a smaller dimensional latent space and a decoder that recovers the original input the encoder projects. The model is only exposed to normal that is during training, therefore, it can correctly reproduce benign patterns and fail to reproduce an abnormal behavior. Anomalies will be detected by determining the error of reconstruction between the input and the reconstructed output. When the error surpasses a pre-established threshold, the instance of the traffic is said to be anomalous. It is effective in the identification of unknown or zero-day attacks because there is no use of labeled attack data in this approach.

3.3.2. LSTM-Based Model

The LSTM-based system is interested in learning the temporal relationships and the sequence of events of the IoT traffic data. Time-series analysis with Long Short-Term Memory networks is well adapted to the characteristics of time-series because time drives can remember long contextual features and reputations and are capable of vanishing gradient tasks. Under this model, LSTM is trained in series of normal traffic in order to forecast future traffic performance or sequence patterns. Abnormalities are detected when the actual and expected traffic behavior has a significant deviation. This deviation shows that there are abnormal dynamics in time, e.g. abrupt spikes, abnormally

ISSN: XXXX-XXXX
PP: 53-65.

persistent irregular activity, or synchronized attacks. LSTM-based method improves the detection of time-scholarly and changing anomalies that are typically evidenced in the internet of things systems.

3.4. Training and Optimization

The training and optimization procedure is an essential part of the suggested framework of anomaly detection since it has a direct impact on the accuracy, resilience, and the generalization potential of the deep learning models. The models are trained with the Adam optimizer that is highly relevant in the process of optimization because it has an adaptive learning rate and can effectively work with sparse gradients. Adam incorporates the strengths of momentum-based optimization as well as adaptive learning methods with the ability to converge faster and better-stabilize at large scale when training deep neural networks on large-scale IoT traffic data. The categorical cross-entropy loss function is used to define the distance between the predicted and actual class labels and is therefore appropriate within the multi-class classification mode since traffic can be classified as normal and other anomalous classes. A number of regularization methods are introduced in the training to reduce overfitting and make the model more generalized. During each training step, dropout selects a random subset of neurons and deactivates them to ensure that the model is neither overdependent on a single feature or set of network connections. This makes the network learn stronger and dispersed feature representations. Besides this, early stopping is also introduced to keep a check on the validation performance and to terminate training in situations where no additional benefit of the training is realized along a set number of epochs. This will avoid over training and the possibility of the model overly committing to noise or outliers in the training data. When performing the optimization, the training dataset is usually split into two subsets training and validation to guarantee objective performance evaluation. Learning rate, batch size, number of epochs, and dropout rate among the hyperparameters are set to the most optimal value to offer the most efficient learning and detection compromise. The proposed models can be used to detect anomalies in the real-world scenario of the IoT with high reliability and scalability, and they can provide improved convergence and reduced overfitting as a result of this systematic training and optimization strategy and exhibit better adaptation to the changing patterns of IoT traffic.

3.5. Real-Time Deployment Strategy

The real-time deployment program of the proposed anomaly detection framework is founded with the objective of providing low latency, scalability, and resource optimization in the IoT settings. In order to attain these goals, edge computing is used to conduct anomaly detection inference near data sources, e.g. Information technology gateways, edge servers, or fog nodes. The framework greatly lowers the communication latency by transferring the computational operations off the centralized cloud servers and to the network edge, as well as reduces the bandwidth requirements to transmit vast quantities of raw IoT traffic. This is especially essential to applications that require quick detection and response to anomalies that would be time-sensitive and require extra features on security. Under the proposed architecture, the data acquired by the IoT devices are preprocessed at the edges and sent to the trained deep learning models and inferred. This decentralized processing also allows the detection of bad or suspicious behavior in close to real time with no continuous

ISSN: XXXX-XXXX
PP: 53-65.

dependency on cloud connectivity. The edge-based inference also increases the reliability of the system because the mechanism of anomaly detection can act even in the conditions where the network is not connected regularly or the capacity of the backhaul is low. Also sensitive data are kept nearer to their source which enhances privacy and limited vulnerability to data incompatibility. In order to save on resource demands of edge devices, model optimization methods can be used, which include model compression, model quantization and lightweight architectures. Such optimizations minimise memory utilisation, and minimise the computational load, without a significant loss in detection accuracy. Besides, the structure is capable of scaling to large-scale deployment by balancing detection loads among network edge nodes, thereby managing more and more IoT devices. Anomalies and summarized alerts are identified and only proportionally sent to centralized management systems or cloud platforms to be analyzed, visualized and stored long-term. In general, the edge-enabled real-time deployment plan contributes to the responsiveness, scalability, and practicability, which makes the suggested framework of anomaly detection to be appropriate to the IoT security real-world application.

4. RESULTS AND DISCUSSION

4.1. Experimental Setup

Well-known benchmark datasets on IoT intrusions detection were used as the experimental methods of the proposed anomaly detection framework to ensure the reliability, reproducibility, and even compare the approaches employed. These datasets are a mix of different normal and malicious traffic patterns that reflect the workings of a real world IoT system, including many different kinds of attacks, such as, denial-of-service, probing, spoofing, and unauthorized access attacks. Assessment with the benchmark datasets can be done using standardized evaluation, and the results of the proposed models can be compared with those that had previously been reported in the literature. The datasets were preprocessed before experimentation so that they fit into the requirements of the framework that was proposed. This involved normalizing the data features, cleaning of data and time segmentation to guarantee consistency between training and testing modes. The data were subsequently separated into training, validation and test data to test how the models can extrapolate to unknown data. The obtained deep learning models utilized earlier in this paper were optimized using training: on the training data, hyperparameter optimization and early stopping were applied to avoid overfitting.

In order to fully evaluate the functionality of the proposed approach, several performance measures were used, such as accuracy, precision, recall, as well as F1-score. The accuracy measures the general accuracy of the model predictions where as the precision evaluates the percentage of correctly detected anomalies of the total anomalies detected. Recall, in other words detection rate, measures the capacity of the model to detect real instances of anomalies, and this is very important in security. F1-score being the harmonic average of recall and precision offers a fair assessment of the ability of the model to detect. Combined, these indicators can provide a powerful and comprehensive evaluation of the framework proposed under consideration in terms of its capability to recognize abnormalities in the IoT network traffic.

ISSN: XXXX-XXXX
PP: 53-65.

4.2. Performance Comparison

Table 1: Performance Comparison

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score
SVM	89.2	87.5	85.1	86.3
Random Forest	91.6	90.2	88.9	89.5
Autoencoder	95.4	94.1	93.7	93.9
LSTM	97.1	96.3	95.8	96.0

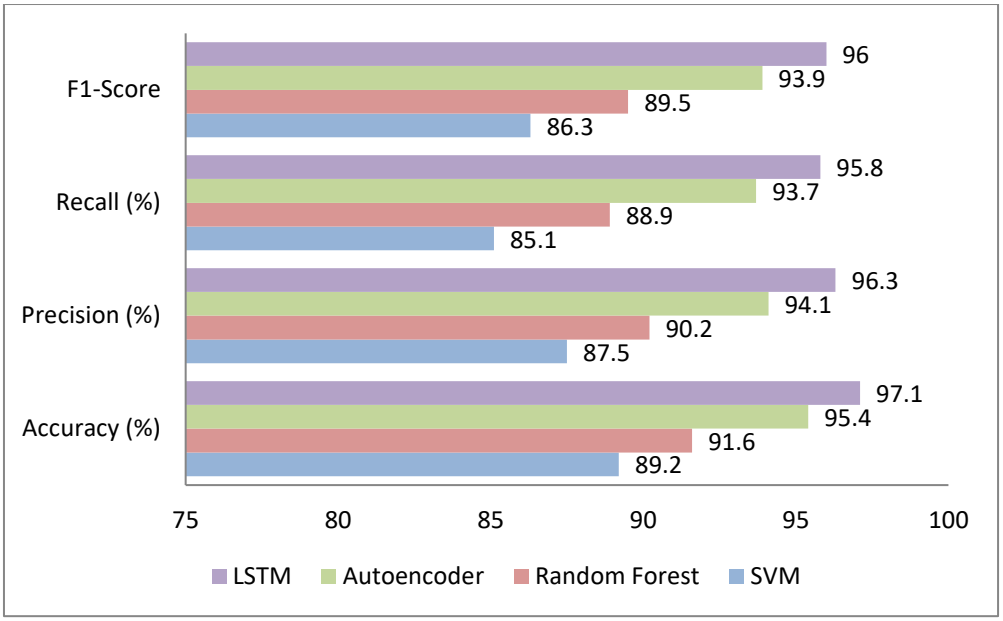

Fig 4 - Graph Representing Performance Comparison

4.2.1. Support Vector Machine (SVM)

The Support Vector Machine model has a mediocre result in the detection of anomalies in the IoT traffic, with the accuracy of 89.2. It has a precision of 87.5 percent showing that it can identify abnormal cases reasonably well, with its recall being 85.1 percent which implies that it is not able to identify all the abnormal cases. The F1-score of 86.37 indicates a trade-off that is balanced but with a restricted level of precision and recall. The effectiveness of SVMs will not be as good in complex and high-dimensional environments of the Internet of Things because they are limited by scalability and use handcrafted features.

4.2.2. Random Forest

Random Forest model is better than SVM as it has an accuracy of 91.6, which also shows that the model better represents the nonlinear relation and feature interactions. Having precision of 90.2 and recall of 88.9, the model is more consistent in detection of normal and anomalous traffic. The F1-score is 89.5% which is an improved overall detection readily than the traditional machine learning methods. Nevertheless, the Random Forest models can be computationally-intensive and fail when deployed in real-time on resource-limited IoT.

ISSN: XXXX-XXXX
PP: 53-65.

4.2.3. Autoencoder

The model based on Autoencoders offers much greater results, and the accuracy rate is 95.4. It has a high precision (94.1) and recall (93.7) and is observed to clearly differentiate abnormal and normal behavior patterns. The maximum F1-score of 93.9 percent explains a balanced performance of detection especially to never encountered attacks or those that are zero-day. This enhancement indicates theusefulness of unmonitored deep learning in learning compressed representations of nonattack traffic of IoTs without using labeled attack data.

4.2.4. LSTM

The LSTM-based model is the most optimistic in the whole set of approaches, and the model has an accuracy of 97.1%. Good precision (96.3), and recall (95.8) thereof represent tremendous ability to detect anomalies with few false positives and false negatives. The F1-score 96.0% indicates the high extent to which the model can model temporal variation and changing trends of traffic trends in the IoT setting. These findings indicate that LSTM networks can be specifically useful in time-series-based anomaly detection and real-time usage in IoT security.

4.3. Discussion

According to the results of the experiment, it is obvious that deep neural network models are much more efficient than the traditional machine learning models to detect anomaly in IoT settings. Support Vector Machines and Random Forests classical models are much based on designed features, and their predetermined decision boundaries which restrict adaptation to complex high dimensional evolving patterns in IoT traffic. Unlike their counterparts, though, deep learning models have the advantage of automatically discovering hierarchical features representations on their own directly out of the data, allowing them to reveal subtle and non-linear relationships that are typically indicative of more complex cyber-threats. This ability is indicated by the significant best in accuracy, precision, recall, and F1-score of an auto-encoder and LSTM-based model. LSTM-based models are the most superior in the set of deep learning methods tested including real-time detection. IoT traffic characteristics are sequential and time sensitive and several attacks have temporal qualities including slow growth over time, periodic bursts or phase coordinated action. LSTM networks are especially formulated to address such dynamic (temporal) relationships by keeping the long-term contextual information which makes them more competent to differentiate between natural variations and the actual anomalies. Such awareness of time leads to an increase in the rate of recall so that fewer locations of malicious activities escape being noticed, which is very important in security sensitive applications. Autoencoders based models work remarkably well as well, particularly in identifying attacks that were never seen before or in zero-day attacks since they do not use known attack signatures, rather they learn normal traffic behaviours. They can however have a slight limitation in terms of their performance in cases where anomalies have similarity of occurrence to the normal over short periods. Altogether, the results point to the fact that deep representation learning and the introduction of the temporal modeling stages can substantially increase detection sustainability and flexibility. These findings highlight the significance of significantly deep neural designs, most

ISSN: XXXX-XXXX
PP: 53-65.

notably, LSTM designed models in the creation of scalable, precise and real-time anomaly detectors that integrate well into the current IoT networks.

5. CONCLUSION

In this paper, I offered a thorough research on real-time anomaly detection in IoT networks with deep neural models, to solve one of the crucially important security concerns related to the active expansion and dynamic increase of IoT ecosystems. The suggested model combines effective data collection, powerful preprocessing, deep learning models, and edge deploy solutions to make anomalous behavior in time and with accuracy. The heterogeneous nature of the IoT devices, the different traffic patterns, and resource limitations characterize the framework in such a way that it can work well in real-life conditions where the conventional security measures do not usually work.

The proposed deep learning-based IoT intrusion detection method showed great performance increase after intensive experimental analysis of benchmark IoT intrusion detection datasets compared to traditional machine learning methods. Models like LSTM networks and autoencoders had better accuracy, precision, recall and F1-score, indicating that they were capable of learning non-linear, complex, and time-dependent patterns in IoT traffic data. Specifically, the LSTM-based model demonstrated an excellent behavior in real-time under conditions, when the temporal dependencies and the changing behavior of attacks are to be considered. These findings confirm that deep neural architectures can be efficient in dealing with many high-dimensional data, concept drift and zero-day attacks that are not easily addressed by rule-based or shallow learning approaches.

Moreover, edge computing implementation on real-time deployment increases the feasibility of the offered framework by lowering the latency, decreasing bandwidth use, and improving privacy of data. Conducting the inference when the data are higher enables quicker detection and reaction, which is needed in reducing security risks in mission-critical IoT uses. The strength of the system is further enhanced by the adaptation and optimization of training measures, regularization, and scalability which enhances the stability and the flexibility of the system.

REFERENCES

[1] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58.
[2] Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12), 3448–3470.
[3] Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, SE-13(2), 222–232.
[4] Lakhina, A., Crovella, M., & Diot, C. (2005). Mining anomalies using traffic feature distributions. ACM SIGCOMM Computer Communication Review, 35(4), 217–228.
[5] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.
[6] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
[7] Nguyen, T. T., & Reddi, V. J. (2020). Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems, 31(9), 3748–3760.
[8] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700.

ISSN: XXXX-XXXX
PP: 53-65.

[9] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. EAI Endorsed Transactions on Security and Safety, 3(9), 1–6.

[10] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961.

[11] Kim, J., & Cho, S. (2019). Deep CNN-based intrusion detection system for IoT. Applied Sciences, 9(13), 2714.

[12] Malhotra, P., Vig, L., Shroff, G., & Agarwal, P. (2015). Long short-term memory networks for anomaly detection in time series. ESANN, 89–94.

[13] Sakurada, M., & Yairi, T. (2014). Anomaly detection using autoencoders with nonlinear dimensionality reduction. Proceedings of MLSDA, 4–11.

[14] Marchal, S., François, J., State, R., & Engel, T. (2014). PhishStorm: Detecting phishing with streaming analytics. IEEE Transactions on Network and Service Management, 11(4), 458–471.

[15] Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer internet of things devices. IEEE Security and Privacy Workshops, 29–35.

[16] Kapadia, H. P. C. (2025). Real-Time Monitoring of Employee Web Activity for Compliance in Banks. Journal Of Advance And Future Research, 3(1), 91-96.