

Securing the internet of things frontier: a deep learning ensemble for cyber-attack detection in smart environments

Deepa Venkataraya Premalatha^{1,2}, Sukumar Ramanujam³

¹Department of Electronics Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India

²Department of Electronics and Communication Engineering, Government Engineering College, Ramanagara, India

³Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India

Article Info

Article history:

Received Feb 8, 2024

Revised May 13, 2024

Accepted Jun 1, 2024

Keywords:

Cyber-attack

Deep learning

Ensemble technology

Internet of things

Intruder detection systems

ABSTRACT

This study presents a novel and innovative approach using deep learning (DL) ensemble technique to improve the security of internet of things (IoT) by identifying intricate cyber-attacks. By utilising advanced DL models like deep neural network (DNN) and long short-term memory (LSTM), our approach significantly enhances the accuracy of categorization compared to basic models. The initial binary classifier achieved an accuracy of 85.2%, while the multi-class classifier achieved an accuracy of 79.7%. Both classifiers continually enhanced, achieving accuracies of 99.34% and 98.26%, respectively, after 100 epochs. Real-time scenario evaluations showed that the average execution time per sample record was 0.9439 ms, confirming its efficiency. The DL ensemble exhibited improved performance in comparison to traditional models, indicating its potential for wider implementation in IoT security. The study not only emphasises significant improvements in accuracy, but also emphasises the method's ability to perform well across many evaluation measures. This study presents a thorough and pragmatic method for identifying cyber-attacks in IoT settings. The stacked ensemble technique outperforms earlier models and fulfils real-time processing requirements, offering substantial advancements in IoT security. These findings enhance both the theoretical comprehension and practical application, establishing a novel benchmark for protecting intelligent IoT systems.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Deepa Venkataraya Premalatha

Department of Electronics and Communication Engineering, Government Engineering College

Ramanagara, Karnataka, India

Email: deepa.venkataraya@gmail.com

1. INTRODUCTION

The advent of the internet of things (IoTs) in the modern digital age has brought about unparalleled progress in connectivity and automation, which has revolutionised traditional spaces into intelligent and adaptable environments. Smart environments facilitated by the IoT integrate sensors, actuators, and devices in a seamless fashion to form a networked ecosystem capable of accumulating, processing, and exchanging vast quantities of data. Nevertheless, this profound potential is not devoid of obstacles, given that the heightened interconnectivity also creates pathways for cyber threats and assaults. With the increasing dependence on interconnected devices, it becomes crucial to prioritise the protection of the IoT frontier to guarantee the availability, confidentiality, and integrity of sensitive data. In the face of unforeseen threats or external assaults, it is imperative that critical infrastructure components, including “internet industrial control systems and sensitive industrial plants and sites (SIPS)”, retain their functionality and reliable operation [1]. Engineers have

purposefully engineered a multitude of systems to mitigate the potential repercussions that could result from the failure or intentional destruction of critical infrastructure. However, these specialised systems remain vulnerable to cyber threats and assaults. SIPS protection is required in both the physical and virtual domains, comprising the management, control, and communication layers, due to its expansive attack surface. With the intention of unlawfully obtaining or modifying sensitive data, attackers endeavour to penetrate these layers using physical, remote, or a combination of attack vectors. Regarding transmission, SIPS is susceptible to cyberattacks. Cyberattacks have the capacity to compromise remotely operated devices, which may cause substantial damage to tangible assets and generate extensive financial losses. Servers containing sensitive data are likely to be of interest to hackers. Moreover, hackers may attempt to alter vital metrics supplied to administrators, thereby affecting the monitoring and control of infrastructure components.

Safeguarding against various layers of potential attacks is a crucial aspect of cybersecurity, encompassing defence mechanisms against malware [2]. Malicious code embedded within software often lies dormant during system inspections, evading detection. These infected systems can establish connections with other compromised systems, forming a botnet that enables cybercriminals to conduct various illicit activities such as distributed denial of service (DDoS) attacks, spam dissemination, ransomware deployment, and surreptitious data exfiltration. The evolution of intrusion detection methods has shifted from reliance on port scanning to the adoption of advanced machine learning (ML) techniques [3]. Modern approaches have surpassed traditional port-based methods, adapting to dynamic port allocation rather than fixed port numbers. With the prevalence of encrypted traffic, traditional payload-based strategies have become less effective. Consequently, there is a growing inclination among cybersecurity experts to employ ML techniques and analyse network flow patterns to enhance detection capabilities.

The advent of the IoT has introduced an unparalleled level of connectivity and efficiency, as it has become an integral part of our everyday existence. Nevertheless, this intricate network of devices also presents an array of security concerns, which necessitates a thorough analysis of the susceptibilities intrinsic to intelligent environments. The exponential expansion of various IoT devices, spanning from personal electronics to industrial sensors, gives rise to an intricate ecosystem in which conventional security protocols are inadequate [4]–[6]. Significant vulnerabilities in the form of sophisticated ransomware attacks and unauthorised access present formidable challenges to the confidentiality and integrity of IoT systems. Consequently, the imperative for resilient cybersecurity solutions that are precisely customised to the ever-changing characteristics of IoT environments arises. Conventional security methodologies, which were originally developed to operate in computing environments that are more conventional in nature, encounter difficulties in effectively tackling the distinct challenges presented by IoT ecosystems. The vast variety of devices and the scarcity of resources necessitate the development of novel approaches [7]. As a subset of ML, deep learning (DL) arises as a potentially effective method for enhancing IoT security. DL is highly suitable for anomaly detection and cyber threat identification in the dynamic and complex environment of smart systems due to its ability to recognise intricate patterns and adapt to evolving threats [8], [9]. This article examines the historical context of security challenges on the IoT, highlights the shortcomings of current security measures, and justifies the implementation of a DL Ensemble strategy to fortify the IoT frontier against cyber-attacks.

The importance of security in the IoT extends beyond technological progress and influences every aspect of contemporary society. As the IoT integrates more deeply into our everyday existence, the risks and complexities surrounding its security escalate at an exponential rate. The fundamental nature of the IoT is the smooth interconnection and discourse among an extensive assortment of devices, encompassing intelligent household appliances as well as vital industrial sensors. While these interrelated systems optimise operations, streamline procedures, and offer unparalleled convenience, they also establish a complex network of susceptible points of failure that are prone to exploitation. The critical importance of IoT security becomes apparent when one contemplates the possible ramifications of breaches occurring within these interdependent ecosystems. Unauthorized access to personal data or control over household devices can result in privacy infringements, identity theft, and even physical security risks in the context of smart homes. The compromise of critical infrastructure via IoT devices in industrial settings can result in severe repercussions, threatening national security, public safety, and economic stability.

Furthermore, due to the interconnectivity of IoT systems, a security vulnerability in a single device can potentially compromise the integrity of the entire network via a cascading effect. Interdependence emphasises the critical nature of establishing strong security protocols to protect against cyber threats. Considering society's ongoing adoption of the IoT, it is crucial to acknowledge and confront the importance of IoT security. This is not solely a technological necessity but rather a fundamental prerequisite for safeguarding the confidence, dependability, and long-term viability of our progressively interconnected global community. The ramifications of security lapses in the IoT on society emphasise the necessity for all-encompassing, proactive, and flexible security approaches to reduce vulnerabilities and protect the integrity of our interdependent future.

This research endeavours to tackle the difficulty associated with devising a proficient anomaly-based approach for network intrusion detection. A comprehensive investigation of current benchmark datasets, specifically IoT-23, LITNET-2020, and NetML-2020, is undertaken with the objective of attaining optimal precision while minimising computational intricacy. The primary aim of this study is to develop an effective anomaly detection system that satisfies the predetermined standards: i) to perform an exhaustive analysis of the existing security flaws in smart environments enabled by the IoT; ii) emphasize the need for more adaptable and resilient solutions while identifying limitations and gaps in the current methodologies; iii) to develop and use a dimensionality reduction algorithm, like deep sparse auto encoder (DSAE), with the goal of reducing the dimensions of the classifier's input feature vector. This is done to reduce computational complexity; iv) to evaluate the efficacy of the proposed DL ensemble model through extensive experiments and assessments.

The manuscript extensively examines the designated contribution. In section 2, a thorough analysis of existing literature related to the subject is conducted. Section 3 introduces an intrusion detection platform based on anomalies, detailing its data preprocessing methods, techniques for feature engineering, and proposing a stacked ensemble ML approach. Section 4 presents findings from experimental investigations. Lastly, section 5 presents conclusions drawn from the study and explores potential avenues for future research.

2. BACKGROUND

This literature analysis began with a thorough examination of the present status of IoT security, a dive into existing cybersecurity solutions, and the emergence of threats in smart environments. In addition, investigated the use of DL in cybersecurity, focusing on its potential to improve anomaly detection and threat identification. Many scholarly contributions have been evaluated to get inspiration and address the challenges related to access control, authentication, application security, encryption, and network security in IoT contexts. A comprehensive assessment reported in [10] thoroughly investigates security risks linked to IoT connectivity, providing insights into widespread difficulties, and proposing alternative remedies. IoT systems are frequently found to be unprepared, providing a chance for hostile actors. In such cases, fraudsters use wireless networks to connect to IoT devices, giving them physical access to critical data [11]. IoT systems are vulnerable because of their sophisticated structure and integrative setups, emphasising the necessity for effective security measures to protect against unauthorised access and potential data breaches. Furthermore, because of the extensive interactions and interdependencies inherent in these systems, the IoT architecture presents new attack surfaces [12]. These traits help to shape the formation of various sorts of assaults. As a result, the security difficulties confronting IoT systems outnumber those confronting traditional computing devices, raising the amount of risk associated with defending these networked ecosystems. Because of the vulnerabilities inherent in IoT systems, complex and possibly destructive assaults, such as the Mirai disaster, are expected to arise. Given the wide range of IoT situations and applications, choosing the most effective IoT security solutions is a significant difficulty. As a result, the major focus of our research is on developing appropriate ways for improving IoT security while addressing the intricacies and dynamic nature of the threat landscape in these networked systems [13].

Various solutions for navigating the junction of security and privacy challenges within the areas of DL and ML have been developed. The most often used methods for safeguarding privacy in the context of DL and ML include homomorphic encryption, differential privacy, trusted execution, and secure multiparty computing environments [14]. Abdallah *et al.* [15] provided a concise overview of the implementation of ML methods in the context of the IoT, with a particular emphasis on data security and privacy protection. These authors' survey identified three key challenges related to the implementation of ML in IoT environments: concerns about communication and computation overhead, the limitation of partial state consideration, and the requirement for robust backup security justifications.

2.1. Smart environments driven by the internet of things

A smart environment refers to a setting where sensors and computational devices seamlessly interact with everyday objects, communicating via a network. This integration aims to enhance human life by improving comfort and efficiency. According to Latif *et al.* [16], smart environments leverage information and communication technologies to enhance awareness, interactivity, and efficiency across various sectors, including city administration, education, healthcare, public safety, real estate, transportation, and utilities. The IoT plays a crucial role in enabling intelligent ecosystems like smart cities, advanced healthcare systems, and efficient building management. The objective of smart environments is to deliver services by leveraging data from IoT-enabled sensors and employing intelligent techniques, impacting various aspects of our lives, including social, commercial, and economic components [17]. Figure 1 illustrates the growth of networked IoT devices and the global IoT market [18], providing insights into economic implications and anticipated industry effects, including the projected market share of major IoT applications by 2025.

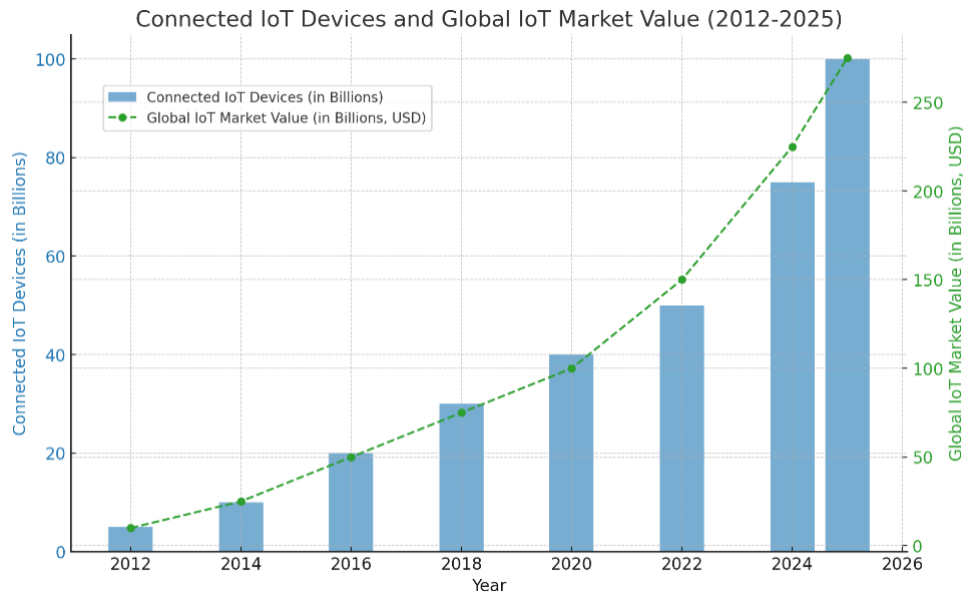


Figure 1. Connected IoT devices vs global market value

2.2. Safety and security threats

The IoT connects physical items and their environs via internet connections. These gadgets often function in an uninvited and sometimes dangerous internet environment. As a result, there is a danger of hostile actors infiltrating and exploiting susceptible IoT devices. Through eavesdropping, this attack might result in the unauthorised disclosure of sensitive information and credentials from sensors [19]. Figure 2 depicts possible security risks that have the potential to influence several securities criteria, such as authorization, authentication, confidentiality, availability, integrity, and non-repudiation.

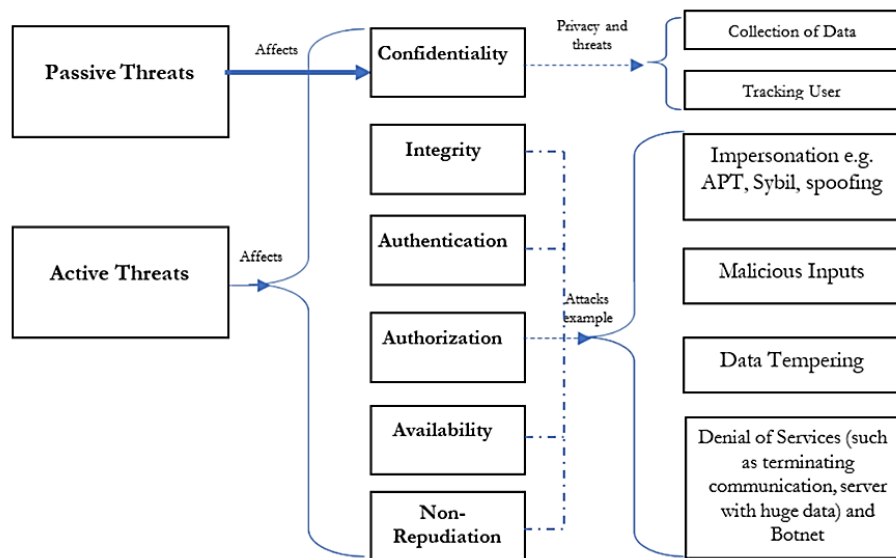


Figure 2. Types of IoT security threats [18]

Furthermore, numerous studies raise serious concerns about the distribution of updates across the large network of billions of smart devices. The inherent computing limits of IoT devices severely limit their ability to effectively mitigate and respond to sophisticated cyber threats. This highlights the significant hurdles connected with ensuring these devices have the necessary capability to smoothly accept and deploy application

upgrades in an efficient manner. In essence, one can divide the vulnerabilities in IoT systems into two categories: those inherent to the devices themselves, and those resulting from the pervasive challenges surrounding their ability to adequately accommodate and execute updates required for security and functionality.

2.3. Deep learning, ensemble learning

DL and deep neural networks (DNN) play a pivotal role in ML, fueled by the emergence of potent graphics processing units (GPUs) boasting remarkable processing power. This technological evolution has significantly impacted artificial intelligence (AI), engineering, and computer science, with a burgeoning influence anticipated in cybersecurity. Although the integration of DNNs into intrusion detection systems (IDS) is still nascent, a mounting body of evidence underscores their potential in fortifying cybersecurity defenses. Laghrissi *et al.* [20] employed long short-term memory (LSTM) networks and evaluated them on the KDD-Cup '99 dataset. The LSTM-recurrent neural network's (RNN) layer model demonstrated strong performance, achieving an accuracy of 96.93% and a recall rate of 98.88%. Similarly, Brunner *et al.* [21] explored the efficacy of deep autoencoders in intrusion detection within big data contexts. Utilizing the NSL-KDD test set, the study aimed to capture essential characteristics via dimensionality reduction, yielding promising accuracy results suitable for real-world intrusion detection applications. Furthermore, Brunner *et al.* [22] conducted comprehensive evaluations on the utility of deep belief networks (DBN) for intrusion detection. Training the DBN using NSL-KDD data enabled the detection of previously unknown threats, showcasing the efficacy of this approach. The proliferation of advanced hardware resources and enhanced computational capabilities of GPU cards have bolstered the adoption of DNN methods as a compelling alternative to conventional intrusion detection approaches.

Researchers used feedforward neural networks (FNN) to develop a new solution for intrusion detection and traffic monitoring within a network in [23]. The Bot-IoT dataset was used in the study for a comparison with the support vector classifier (SVC). Experiment results showed that the FNN model outperformed, attaining a remarkable accuracy of 99.414% in multi-class categorization of DDoS/DoS assaults. Furthermore, the FNN model outperformed all other assessment measures, including accuracy, precision, recall, and F1 score, with an overall effectiveness of 0.99%. According to Ge *et al.* [24], traditional IoT security strategies primarily focus on identifying threats that originate from either the device or the cloud. However, this technique limits the capacity to identify a variety of malicious activities, such as botnet infiltrations, phishing attempts, and DDoS assaults among IoT devices. On the other hand, it presented a revolutionary cloud-based detection solution based on DL methodologies. They suggest the use of distributed convolutional neural networks (DCNN) for IoT devices and LSTM for cloud backend hosts, therefore solving the weaknesses of existing security paradigms.

Stacking, or stacking generalisation, is a method that can significantly improve the performance of ML models. This strategy produces an overall gain in performance by utilising a meta-classifier to combine the predictions made by various models [25]. Papamartzivanos *et al.* [26] combined hidden Markov and naive Bayesian models to improve the flexibility of IDs. The study's findings demonstrated that employing this stratified generalisation strategy produced positive benefits. Balancing accuracy with low false alarms in IoT traffic security, particularly in the realm of DL, is difficult. This problem is especially acute at CNNs. Furthermore, using FNN for multi-class classification limits the efficiency of IoT network security against information theft and key logging, with optimal effectiveness confined to binary classification techniques. In the suggested paradigm, a third constraint emerges, appearing as a performance reduction in IDS during periods of high network traffic. These constraints highlight the need for sophisticated ways to handle the complexities of IoT security enhancement.

3. PROPOSED METHOD

The major goal of this research is to generate reliable outlier classifications using a sophisticated stacked ensemble technique. The following section will provide readers with an extensive description of the framework used in this study. Following the framework overview, an in-depth examination of the complexities of data pre-processing, feature engineering, and the subsequent stages involving classifier modelling will be meticulously explored.

3.1. Dataset of cyber-attacks

Data collection requires obtaining information about certain variables within a dataset in a methodical manner. This methodical methodology makes it easier to investigate defined research topics, scrutinise stated hypotheses, and assess outcome consequences. The focus of data collection in this study is on factors linked to intrusions and assaults on data records in IoT computing systems. Several flow-based benchmark datasets, such

as IoT-23, LITNET-2020, and NetML-2020, have been made public. Despite their recent release, these datasets have received little attention from the cybersecurity community. This research utilized these datasets to perform effective anomaly-based network intrusion detection. This enables us to analyse and find abnormalities in realistic and current network traffic data, offering useful insights on the effectiveness of our IDs on current datasets. The IoT-23 dataset, which can be found at “<https://www.stratosphereips.org/datasets-iot23>”, has 20 malware subsets and three benign subsets inside network traffic. This dataset was initially provided in January 2020 by the “Stratosphere Laboratory in Czechia”. Its major goal is to provide a large collection of labelled data, which includes both malware and benign network traffic collected from legitimate captures. The goal is to make it easier to design intrusion detection technologies, particularly those that use ML methods. The dataset contains 21 feature traits, including nominal and quantitative properties, as well as timestamps. These properties define each data instance, including a class name that specifies the type of connection. Table 1 offers an in-depth analysis of the dataset, highlighting the many properties connected to each data point. The study then goes on to explain the attack class labels, providing a full overview of the many sorts of security risks contained in the dataset. Because of the large size of the IoT-23 dataset, this study focused on a small collection of five scenarios for evaluation.

Table 1. IoT-23 datasets used

| Sl. No. | Malware detail | Capture detail |
|---------|----------------|----------------|
| 1 | Hide&Seek | Malware-1-1 |
| 2 | Bening | Honey-pot-4-1 |
| 3 | Bening | Honey-pot-7-1 |
| 4 | Mirai | Malware-34-1 |
| 5 | Mirai | Malware-43-1 |

LITNET-2020, the NetFlow dataset utilised in this investigation, is available at <https://dataset.litnet.lt>. It comprises senders and receivers. The senders, which are comprised of Cisco routers and FortiGate firewalls, are strategically positioned to monitor the passage of NetFlow data through the assigned collectors. Software specifically developed for the reception, storage, and filtration of data is installed on these collectors. The dataset comprises a grand total of 45,492,310 fluxes, the quantities of which are detailed in Table 2 for each class. The classifications in question incorporate both benign and malevolent data, with the former comprising 45,330,333 flows and the latter 5,328,934 flows. The latter is additionally categorised into nine classifications, which correspond to distinct varieties of network intrusions.

Table 2. LITNET-2020 datasets used

| Flows | Attacks (%) | Attack types |
|------------|-------------|-----------------------------|
| 3,994,426 | 1.48 | Smurf |
| 3,863,655 | 0.3 | ICMP-flood |
| 606,814 | 9.8 | UDP-flood |
| 14,608,678 | 25.5 | TCP SYN-flood |
| 3,963,168 | 0.58 | HTTP-flood |
| 3,569,838 | 1.47 | LANDattack |
| 2,858,573 | 0.85 | Blaster worm |
| 5,082,952 | 24.7 | Code red worm |
| 1,153,020 | 0.065 | Spam bot's detection |
| 4,377,656 | 0.027 | Reaper worm |
| 6687 | 93.2 | Scanning/spread |
| 1,244,866 | 0.038 | Packet fragmentation attack |

3.2. Overview of proposed architecture

In this section, a complete, deep-stacked ensemble approach for detecting anomalies in network traffic data is discussed. Figure 3 shows a graphic representation of the complicated construction. The framework is divided into five stages: i) meticulous dataset selection; ii) data preprocessing; iii) data output; iv) data splitting; and v) classification into “normal/anomaly” categories. This categorization is carried out with the help of a unified stacked ensemble strategy that smoothly integrates deep models and a meta learner. NetFlow files frequently include a variety of feature properties classified as flow, basic, content, time, extra created, and labelled. Nonetheless, packet captures produce a plethora of data, including useless or repetitive information. Extraneous information must be removed to improve the accuracy and impartiality of detection processes. The network traffic datasets have varying magnitudes in their continuous values, which presents difficulties for various classifiers. To address this issue, a scaling procedure is used to normalise the characteristics,

compressing the values between 0 and 1. As a result, the features are scaled according to the concepts indicated in (1). When dealing with variables of varied magnitudes, this normalisation strategy is critical for guaranteeing consistency in the dataset and optimising classifier performance. In the context of our methodology, $\bar{x}_{m,n}$ denotes the normalized feature, where $\max_n(x_{m,n})$ stands for the highest value observed in the data for the m-th feature. The variable i signifies the count of samples present in both the training and testing datasets, while f represents the number of features determined through the feature selection procedure.

$$\bar{x}_{m,n} = \frac{x_{m,n}}{\max_n(x_{m,n})}, \forall m=1,\dots,f, \forall n=1,\dots,i \quad (1)$$

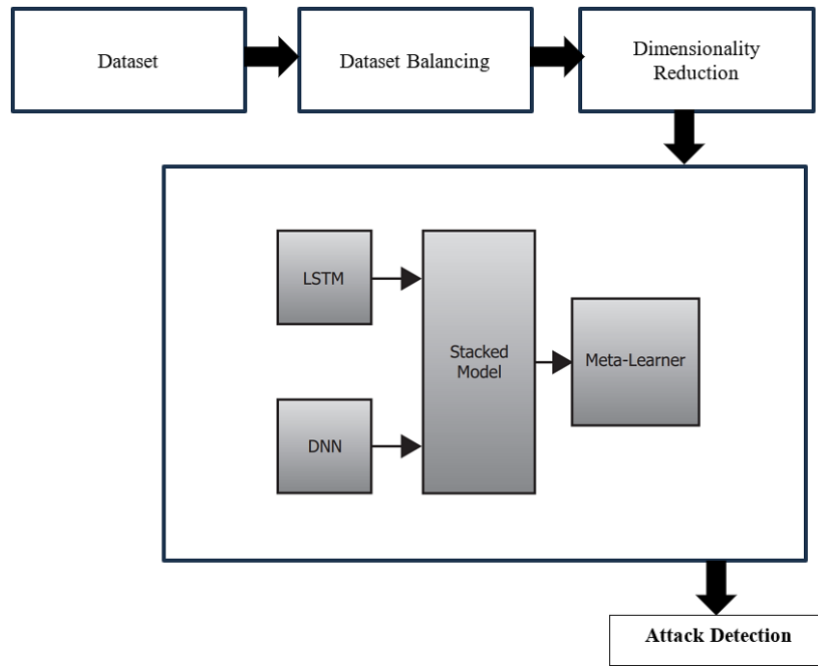


Figure 3. Proposed model architecture

3.3. Data balancing

ML algorithms may meet difficulties when confronted with uneven class distributions within a learning dataset. In the context of unbalanced data learning, addressing this issue frequently entails applying proven procedures, such as under-sampling the majority class. Another approach uses a mix of oversampling and under sampling approaches to generate a more balanced representation of classes within datasets. Adaptive synthetic sampling (ADASYN), a variant of the synthetic minority over-sampling technique (SMOTE), was utilised. The density distribution of distinct locations in the feature space is used by ADASYN to dynamically alter the synthetic sample production. The weight assigned to each instance (w_i) is determined by the density ratio (r_i) and a user-defined parameter β . The purpose of the weight is to emphasize instances in regions with lower density ratios, indicating areas where the class imbalance is more pronounced. The weight is calculated using the formula in (2). The density ratio for an instance x_i in the minority class is calculated by considering the ratio of the number of minority instances among the k nearest neighbors of x_i to the total number of instances among those k -nearest neighbors. ADASYN tries to equalise the distribution of synthetic samples by introducing weights into the synthetic sample generation process, with a stronger emphasis on parts of the feature space where the minority class is underrepresented.

$$w_i = \frac{1}{1+\beta \cdot (1-r_i)} \quad (2)$$

3.4. Dimensionality reduction

The DSAE learning technique is used in the dimensionality reduction process, which employs an autoencoder to extract latent representations of features inside a smaller space. When used unsupervised, the

autoencoder learns to contain the main properties of the input vector. The DSAE distinguishes itself by incorporating a sparse penalty term, a unique addition to the autoencoder idea. This inclusion impedes simple feature learning, forcing the model to achieve a more concise representation of the input vector. The use of DSAE is justified by the aim of creating a rebuilt depiction of the input vector. The DSAE cost function incorporates sparsity to restrict the average activation value across neural nodes in the computational layers. This technique ensures that the encoded representation remains sparse, which helps the model capture important features and accurately reconstruct the input vector.

4. RESULTS AND ANALYSIS

Verification and validation are critical procedures and quality assurance techniques that are carried out independently to check a system's conformity to defined criteria and standards, ensuring that it achieves its intended goals. Verification entails a series of operations aimed at determining the suitability of a system or component, basically checking whether the product is being built appropriately. Validation, on the other hand, includes actions aimed at scrutinising the alignment of the system or its parts with their intended purpose and functions and validating whether the correct product is being generated. Although system validation and verification are independent, their operations are linked and should be carried out together. In this part, a thorough verification and validation process is executed to ensure that the system is aligned with its intended aims and objectives.

4.1. Evaluation and verification metrics

A complete assessment was carried out to examine the effectiveness and alignment of the proposed system with its intended capabilities and aims. The performance of the system was evaluated using the specified testing dataset, with an emphasis on important parameters such as classification accuracy and classification time. This review sought to validate the system's efficacy in accomplishing its objectives.

$$\text{Classification Accuracy (\%)} = \frac{\text{Correctly Predicted Samples}}{\text{Number of Testing Samples}} \times 100 \quad (3)$$

$$\text{Classification Time (ms)} = \sum_{i=1}^{\text{no. of runs}} \text{Execution Time} \times \frac{1000}{\text{no. of runs}} \quad (4)$$

The initial classification accuracy proportions were noticeably low at the start of the testing procedure and after completing one full run (epoch), standing at 85.2% for the two-class classifier and 79.7% for the five-class classifier, as shown in Figure 4. Following that, both classifiers showed an increasing trend in classification accuracy, with a consistent tendency throughout subsequent testing epochs. Particularly, the two-class classifier increased more quickly and significantly, hitting higher ceiling values for classification accuracy. The system demonstrated tremendous progress after 100 epochs of training, reaching an astonishing 99.34% accuracy for the two-class classifier and 98.26% accuracy for the five-class classifier in successfully categorising the given test dataset samples.

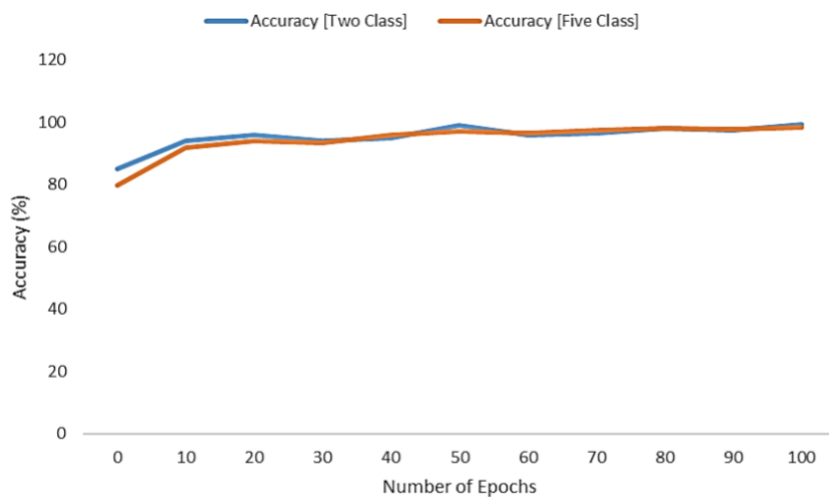


Figure 4. Classification accuracy vs epochs

Furthermore, our research included an in-depth analysis of the time required to execute attack detection or classification on individual IoT traffic samples. The validation test executed 500 times in total to ensure precision and accuracy. Following that, calculated the time statistics for detection and classification. The time range per sample record was 0.5662 to 2.099 ms, with an average time of 0.9439 ms during the 500 simulation iterations, shown in Figure 5. This average time is extremely useful for the system's smooth functioning in dynamic contexts, notably in the context of real-time IDS applications.

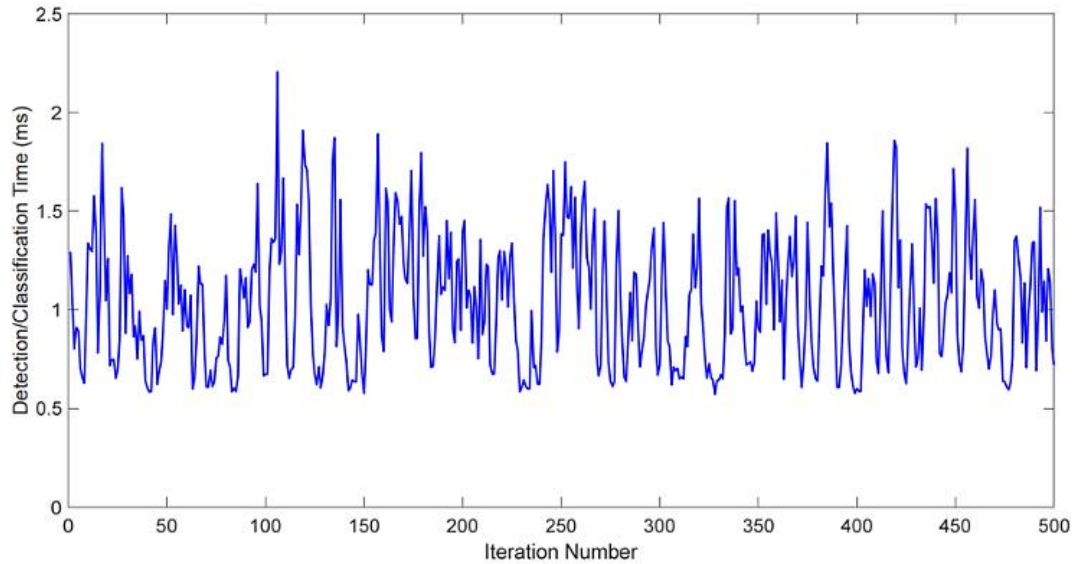


Figure 5. Classification time curve

The g-mean approach, as described in [27], is used in this work to evaluate the performance of classifiers on datasets with an unbalanced class distribution. In such cases, the geometric mean (g-mean) serves as a measure for evaluating classifier outcomes. This technique for assessment is especially useful in the case of unbalanced datasets, ensuring a meaningful and thorough examination of classifier efficacy. Table 3 compares the overall accuracy and achieved g-mean score of the state-of-the-art classifiers to the stacked ensemble classifier.

$$g - mean = \sqrt[M]{\prod_{m=1}^M ACC_m} \quad (5)$$

Table 3. Comparison of accuracy and g-mean of different methods on IoT-23 and LITNET-2020 datasets

| Reference | Method | IoT-23 | | LITNET-2020 | |
|-----------|------------------------|------------------------|--------|-------------|--------|
| | | Accuracy | g-mean | Accuracy | g-mean |
| [28] | Random forest | 89.3 | - | 91.1 | - |
| [29] | Multi-layer perceptron | 98.8 | - | 98.1 | - |
| [30] | Support vector machine | 83.7 (NSL-KDD Dataset) | - | - | - |
| Ours | DL ensemble | 98.3 | 98 | 99.3 | 99 |

As a baseline models, selected two fundamental classification models: DNN and LSTM. DNN, which is extensively used across several domains, and LSTM, which is known for its profound DL capabilities, were chosen for their demonstrated success in making considerable gains in accuracy. This selection stems from an appreciation for these models' adaptability and demonstrated performance in a variety of applications, establishing a strong foundation for the comparative study within the scope of current research. The observed improvements reflect a significant increase in the efficacy of the suggested stacked ensemble approach over the baseline. This method could improve classification accuracy as well as provide favourable results across a variety of assessment parameters.

5. CONCLUSION

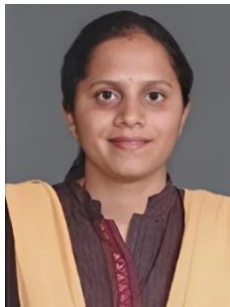
An analysis of a suggested DL ensemble method demonstrates substantial improvements in the accuracy of categorising IoT traffic samples. Although they had originally suboptimal proportions, both the two-class and five-class classifiers shown constant and considerable improvement over the course of testing epochs. Ultimately, they achieved remarkable accuracy rates of 99.34% and 98.26% respectively, after 100 training epochs. The rapid and substantial enhancement, particularly in the two-class classifier, showcases the efficacy of the suggested technique in classifying diverse IoT data. In addition, this study examined the practicality of the system, including real-time IDS applications. After doing more than 500 simulation iterations, the time analysis revealed that the average execution time per sample record was 0.9439 milliseconds. The efficiency of this technology is crucial for its seamless integration in dynamic conditions, enhancing its practicality in real-world scenarios. This study establishes a strong basis for the efficacy of the proposed strategy by conducting a comparative analysis between the DL ensemble method and baseline models, specifically DNN and LSTM, which are well acknowledged for their versatility and DL capabilities. The observed improvements confirm the significant benefits of the proposed technique compared to existing models, showcasing its capacity to enhance classification accuracy and yield favourable outcomes across several evaluation metrics.




REFERENCES

- [1] R. Kozik, M. Choraś, A. Flizikowski, M. Theocharidou, V. Rosato, and E. Rome, "Advanced services for critical infrastructures protection," *Journal of Ambient Intelligence and Humanized Computing*, vol. 6, no. 6, pp. 783–795, Dec. 2015, doi: 10.1007/s12652-015-0283-x.
- [2] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Security issues and challenges for cyber physical system," in *2010 IEEE/ACM Int'l Conference on Green Computing and Communications and Int'l Conference on Cyber, Physical and Social Computing*, IEEE, Dec. 2010, pp. 733–738, doi: 10.1109/GreenCom-CPSCoM.2010.36.
- [3] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in *2016 8th IEEE International Conference on Communication Software and Networks (ICCSN)*, IEEE, Jun. 2016, pp. 581–585, doi: 10.1109/ICCSN.2016.7586590.
- [4] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of things: evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, Mar. 2021, doi: 10.3390/s21051809.
- [5] J. Zhang, H. Chen, L. Gong, J. Cao, and Z. Gu, "The current research of IoT security," in *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, IEEE, Jun. 2019, pp. 346–353, doi: 10.1109/DSC.2019.00059.
- [6] M. Saied, S. Guirguis, and M. Madbouly, "Review of artificial intelligence for enhancing intrusion detection in the internet of things," *Engineering Applications of Artificial Intelligence*, vol. 127, 2024, doi: 10.1016/j.engappai.2023.107231.
- [7] P. Devasis and H. M. Tun, "Security challenges: M2M communication in IoT," *Journal of Electrical Engineering and Automation*, vol. 4, no. 3, pp. 187–199, Oct. 2022, doi: 10.36548/jeea.2022.3.006.
- [8] S. Bharati and P. Podder, "Machine and deep learning for IoT security and privacy: applications, challenges, and future directions," *Security and Communication Networks*, pp. 1–41, Aug. 2022, doi: 10.1155/2022/8951961.
- [9] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions," *Mobile Networks and Applications*, vol. 28, no. 1, pp. 296–312, 2023, doi: 10.1007/s11036-022-01937-3.
- [10] M. Majid *et al.*, "Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review," *Sensors*, vol. 22, no. 6, Mar. 2022, doi: 10.3390/s22062087.
- [11] A. S. L. Kowta, P. K. Harida, S. V. Venkatraman, S. Das, and V. Priya, "Cyber security and the internet of things: vulnerabilities, threats, intruders, and attacks," in *Proceedings of International Conference on Computational Intelligence and Data Engineering*, 2022, pp. 387–401, doi: 10.1007/978-981-16-7182-1_31.
- [12] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of things: evolution and technologies from a security perspective," *Sustainable Cities and Society*, vol. 54, Mar. 2020, doi: 10.1016/j.scs.2019.101728.
- [13] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A comprehensive and systematic survey on the internet of things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures," *Computers*, vol. 9, no. 2, 2020, doi: 10.3390/computers9020044.
- [14] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol. 188, Apr. 2021, doi: 10.1016/j.comnet.2021.107840.
- [15] E. E. Abdallah, W. Eleisah, and A. F. Otoom, "Intrusion detection systems using supervised machine learning techniques: a survey," *Procedia Computer Science*, vol. 201, pp. 205–212, 2022, doi: 10.1016/j.procs.2022.03.029.
- [16] S. Latif, F. F. Dola, M. M. Afsar, I. J. Esha, and D. Nandi, "Investigation of machine learning algorithms for network intrusion detection," *International Journal of Information Engineering and Electronic Business*, vol. 14, no. 2, pp. 1–22, Apr. 2022, doi: 10.5815/ijieeb.2022.02.01.
- [17] J. B. Awotunde *et al.*, "An ensemble tree-based model for intrusion detection in industrial internet of things networks," *Applied Sciences*, vol. 13, no. 4, Feb. 2023, doi: 10.3390/app13042479.
- [18] G. Abbas, A. Mehmood, M. Carsten, G. Epiphaniou, and J. Lloret, "Safety, security and privacy in machine learning based internet of things," *Journal of Sensor and Actuator Networks*, vol. 11, no. 3, Jul. 2022, doi: 10.3390/jsan11030038.
- [19] F. J. Furrer, "Safe and secure system architectures for cyber-physical systems," *Informatik Spektrum*, vol. 46, no. 2, pp. 96–103, Apr. 2023, doi: 10.1007/s00287-023-01533-z.
- [20] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," *Journal of Big Data*, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-021-00448-4.
- [21] C. Brunner, A. Kö, and S. Fodor, "An autoencoder-enhanced stacking neural network model for increasing the performance of intrusion detection," *Journal of Artificial Intelligence and Soft Computing Research*, vol. 12, no. 2, pp. 149–163, Apr. 2021, doi: 10.2478/jaiscr-2022-0010.




- [22] A. M. Banaamah and I. Ahmad, "Intrusion detection in IoT using deep learning," *Sensors*, vol. 22, no. 21, Nov. 2022, doi: 10.3390/s22218417.
- [23] A. Awajan, "A novel deep learning-based intrusion detection system for IoT networks," *Computers*, vol. 12, no. 2, Feb. 2023, doi: 10.3390/computers12020034.
- [24] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks," in *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*, IEEE, Dec. 2019, pp. 256–25609, doi: 10.1109/PRDC47002.2019.00056.
- [25] L. A. Ortega, R. Cabañas, and A. R. Masegosa, "Diversity and generalization in neural network ensembles," *arXiv-Computer Science*, Oct. 2021, doi: 10.48550/arXiv.2110.13786.
- [26] D. Papamartzivanos, F. G. Marmol, and G. Kambourakis, "Introducing deep learning self-adaptive misuse network intrusion detection systems," *IEEE Access*, vol. 7, pp. 13546–13560, 2019, doi: 10.1109/ACCESS.2019.2893871.
- [27] E. Rendón, R. Alejo, C. Castorena, F. J. I. -Ortega, and E. E. G. -Gutiérrez, "Data sampling methods to deal with the big data multi-class imbalance problem," *Applied Sciences*, vol. 10, no. 4, Feb. 2020, doi: 10.3390/app10041276.
- [28] V. Dutta, M. Choraś, M. Pawlicki, and R. Kozik, "A deep learning ensemble for network anomaly and cyber-attack detection," *Sensors*, vol. 20, no. 16, Aug. 2020, doi: 10.3390/s20164583.
- [29] S. K. Katherasala, V. S. Manvith, A. Therala, and M. Murala, "NetMD-network traffic analysis and malware detection," in *2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC)*, IEEE, Feb. 2022, pp. 11–16, doi: 10.1109/ICAIIIC54071.2022.9722691.
- [30] K. A. Taher, B. M. Y. Jisan, and M. M. Rahman, "Network intrusion detection using supervised machine learning technique with feature selection," in *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, IEEE, Jan. 2019, pp. 643–646, doi: 10.1109/ICREST.2019.8644161.

BIOGRAPHIES OF AUTHORS



Deepa Venkataraya Premalatha    received a B.E. degree in Electronics and Communication from Bangalore University, Bengaluru, India, in 2001, M.Tech. degree in Digital Communication and Networking from Visvesvaraya Technological University, Belgaum, India, in 2007. She has worked in Software Company UNISYS Global Services, INDIA as SWE5 (Software Engineer) with 5 years of Industry experience from 2007 to 2011. She has worked in the company with the role of Tester in projects such as Agile Business Suite (Ab Suite) and Performance Benchmark of Ab-Suite Application. TPC-W Benchmarking using JMeter also played the role of developer in projects such as application defender, injection of vulnerabilities in application defender using Java/J2EE technologies. She is currently working as an Assistant Professor in the Department of Electronics and Communication, Government Engineering College, Ramanagara, India with 13 years of teaching experience. Her current research interests are IoT, network security, machine learning, and deep learning. She can be contacted at email: deepa.venkataraya@gmail.com.



Sukumar Ramanujam    received his B.E. in ECE from Madurai Kamaraj University in 1992, M.E. in CSE from Manonmanium Sundaranar University in 2004, and Ph.D. from Anna University in 2010. He has over 25 years of teaching experience. He is also serving as a member of the Board of Studies and various committees. His research areas of interest include cryptography and network security, sensor networks, Cloud, and IoT. He can be contacted at email: r.sukumar@jainuniversity.ac.in.