Journal of Theoretical and Applied Information Technology
15st June 2026. Vol.104. No.11

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

A NOVEL HYBRID FIREFLY ALGORITHM AND LSTM BASED INTELLIGENT SYSTEM FOR IOT SECURITY

S R V PRASAD REDDY[1], K NARAYANA RAO2, DIVESH SINGH SAI[3], MYLAVARAPU KALYAN RAM[4], HANUMANTHA RAO BATTU[5], A MOHAN[6], PULICHERLA SIVA PRASAD[7], VASAVI MANDADI[8]

[1]Department of CSE in Data Science, Dayananda Sagar Academy of Technology and Management, Udayapura, Kanakapura Road, Bangalore, India

[2]Department of CSE, RISE Krishna Sai Prakasam Group of Institutions, Ongole, Andhra Pradesh, India

[3]Senior Software Development Engineer, Amazon, Seattle, Washington, USA

[4]Department of CSE, Aditya University, Surampalem, Andhra Pradesh, India

[5]Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India

[6]Department of CSE, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India

[7]Department of CSE, R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India

[8]Department of CSE, R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India

E-mail: mtechprasadreddy@gmail.com, narayanarao2@gmail.com, Saidivesh92@gmail.com, kalyanram1985@gmail.com, hanuma9999@yahoo.com, amohan_cse@cbit.ac.in, prasadsiva_17@yahoo.com, vasavilahari@gmail.com

ABSTRACT

The extensive adoption of the Internet of Things (IoT) has brought forth numerous potential opportunities and advantages across various facets of our lives. Nonetheless, it is unfortunate that IoT is also associated with various vulnerabilities and a heightened risk of attacks and anomalies. The main objective of these attacks is to unlawfully obtain sensitive information from the system, while simultaneously creating interruptions in system access for legitimate users. This study presents an enhanced Long Short-Term Memory (LSTM) architecture aimed at effectively identifying attacks within an IoT environment. The hyper-parameters of LSTM are optimized using an innovative Memetic Self Adaptive Firefly Algorithm (MAFA). This study presented a perturbation operator and incorporated it into the proposed MAFA to mitigate the risk of local optimum solutions in the conventional firefly method. The comparative assessment of the suggested methodology against other competing deep learning approaches reveals that the proposed method excels across various performance metrics, including F1 score, F2 score, Fbeta score, precision, recall, ROC-AUC score, and accuracy. The MAFA-LSTM methodology demonstrates exceptional performance compared to all other approaches examined, achieving an accuracy of 99.99%. It demonstrates exceptional effectiveness in precisely identifying intrusions within an IoT setting.

Keywords: *IoT, IDS, TON-IoT, MAFA, DL, LSTM*

1. INTRODUCTION

In the realm of technology, the Internet of Things (IoT) is a revolutionary concept that encompasses a vast network of interconnected physical objects or things. All of these things have been outfitted with sensors, software, and communication protocols that have been implanted within them. Utilizing the internet, these devices, which include everything from wearable technology and household appliances to industrial gear and automobiles, collect and share data with one another. Increasing the intelligence and connection of these "things" is the major goal of the Internet of Things (IoT). This will allow these "things" to independently gather information from their surroundings, communicate with other devices, and even respond to commands remotely [1]. By doing so, the Internet of Things gives individuals and businesses the ability to access real-time data, to make decisions based on the data, and to automate processes. This is a

significant contributor to increased productivity, convenience, and innovation in a variety of fields, including smart healthcare, smart homes, smart agriculture, smart industry, and smart transportation [2].

A variety of vulnerabilities have been brought into sectors such as online privacy, social media, corporate functions, and key infrastructure as a result of the rise of cyber threats inside these domains. As a consequence of this, the development of robust techniques has evolved into an essential component inside contexts that are dynamic [3]. The Internet of Things (IoT) is a constantly developing and rising technology landscape that has the potential to significantly alter the security and risk scenario of interconnected automated networks. New cyber dangers have emerged as a result of the increased attack surface that Internet of Things ecosystems present. These vulnerabilities are a result of the increased attack surface. At the same time as these attacks may directly target the Internet of Things devices themselves, they may also utilize Internet of Things devices as a gateway to penetrate other systems. When it comes to the protection of Internet of Things (IoT) infrastructures, intrusion detection systems (IDS) play a crucial part in improving the overall security posture of an IoT infrastructure. The Intrusion Detection System (IDS) is a useful and efficient tool for identifying and preventing prospective assaults, hence enhancing network security and protecting against hostile intruders [4]. In the realm of intrusion detection systems (IDS), anomaly-based algorithms have demonstrated remarkable effectiveness in identifying zero-day attacks, which are attacks that have not been seen before. A set of unplanned acts, whether they take place locally or worldwide, that have the potential to threaten the network's CIA (Confidentiality, Integrity, and Availability) is what we mean when we talk about an incursion. IDS that are built for Internet of Things connected devices use internal mechanisms that are comparable to those shown in Figure 1. Contemporary approaches to anomaly detection, on the other hand, are more adapted to handling growing dangers in dynamic systems of Internet of Things devices. This is in contrast to classic signature-based solutions. When doing an analysis of network traffic, it is necessary to examine packets, including the header fields connected with them, and to extract elements that are pertinent. Identifying and preventing unexpected behaviors, which may include both passive and aggressive actions by intruders, is the primary goal of intrusion detection systems (IDS). This can be accomplished whenever it is possible to do so. By doing so, an intrusion detection system (IDS) helps to reinforce the fundamental concepts that make up the CIA trinity [5].

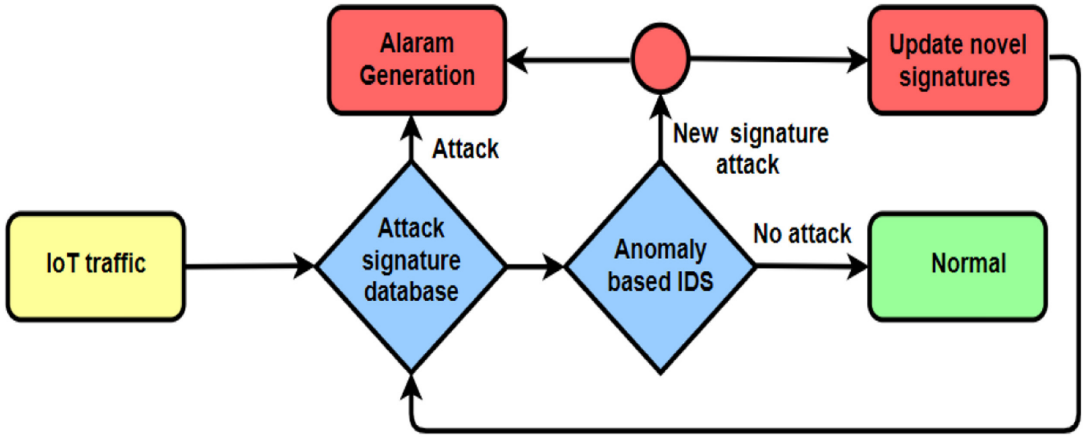

Figure 1. An overview of a general anomaly-based IoT intrusion detection system approach

Datasets in IoT frequently exhibit imbalance as a result of the unique traits of IoT environments. This disparity exists due to the fact that most IoT devices function in standard, non-threatening environments, whereas security incidents happen rarely. As a result, the gathered dataset exhibits this uneven distribution, showcasing a surplus of normal data instances in contrast to the comparatively infrequent occurrences of intrusions or anomalies [6]. The existing imbalance presents significant challenges for the effective training of Machine Learning (ML) models. This situation can result in a bias toward the majority class, ultimately diminishing the model's sensitivity in identifying the minority class, which represents the genuine security threats. Addressing data imbalance via

sampling techniques and feature selection can lead to unintentional information loss or heightened computational demands. The methodologies encounter difficulties in adjusting to the variable characteristics of IoT traffic flow. The IoT environments, characterized by a wide variety of heterogeneous devices and communication protocols, present challenges in selecting the appropriate features due to the diverse nature of these devices and the constantly evolving threat landscape.

Models based on machine learning that are integrated into IoT intrusion detection systems may encounter weaknesses against adversarial attacks, which can hinder the clarity of threat detection. This situation poses challenges to understanding and trusting the decision-making processes of the system. Deep learning outperforms traditional machine learning for intrusion detection systems in the Internet of Things setting primarily due to its ability to efficiently handle complex large datasets and adapt to new security threats as they arise [7]. The environments of the Internet of Things produce extensive and varied data from multiple sources, which complicates the task of accurately identifying anomalies and security breaches. The deep learning algorithms demonstrate significant efficacy in independently acquiring intricate patterns and representations from unprocessed data, without reliance on manually crafted features. This adaptability is essential in IoT environments, where new attack vectors and techniques are constantly evolving. Deep learning models are capable of processing data in real-time, which makes them particularly appropriate for the dynamic and resource-limited characteristics of IoT devices. In summary, deep learning demonstrates superior effectiveness for IoT intrusion detection systems compared to traditional machine learning techniques, owing to its capacity to autonomously identify intricate patterns within the irregular and ever-changing data characteristic of IoT environments. Hyper-parameter tuning holds great importance in the development of IDS models for the IoT. The diversity of IoT environments is notable, characterized by a range of data sources, network topologies, and traffic patterns. As a result, a universal set of hyper-parameters cannot be applied effectively across all scenarios. The importance of hyper-parameter tuning is evident in its capacity to optimize the model's architecture and parameters to align with the unique features of an IoT network [8]. Fine-tuning hyper-parameters can significantly improve the model's precision in detecting intrusions and reducing false positives, which is essential in the realm of IoT. Moreover, the ever-changing landscape of IoT networks necessitates models that can adjust to emerging threats and varying network conditions, rendering hyper-parameter tuning a continuous endeavor to ensure the IDS remains effective over time. By meticulously choosing and fine-tuning hyper-parameters, IoT-based IDS architectures can effectively tackle the specific challenges inherent to IoT environments, thereby enhancing their overall security and reliability.

DL represents a sophisticated approach for improving Network IDS through the thorough analysis of data characterized by intricate structures. Drawing inspiration from biological nervous systems, various deep learning models, including Deep Belief Networks (DBN), Deep Neural Networks (DNN), Recurrent Neural Networks (RNN), and Convolutional Neural Networks (CNN), possess the ability to independently learn intricate, non-linear relationships within data, even in the presence of inconsistencies [9,10]. Nonetheless, these architectural models might face challenges when addressing irregular time-series data within IoT environments and may require additional pre-processing or interpolation techniques to efficiently handle differing time intervals. Furthermore, IoT datasets often require comprehensive pre-processing or manual feature engineering to effectively extract the pertinent data. Data from IoT devices frequently exhibits a sequential structure, resembling time-series data gathered from an array of sensors. LSTM networks are designed to effectively handle sequential data while maintaining long-term dependencies, making them particularly well-suited for analyzing streams of IoT data. The data produced by IoT devices can be influenced by noise resulting from elements like sensor inaccuracies or external environmental interference. LSTMs demonstrate a crucial capacity to adapt to noise, effectively filtering out irrelevant information and emphasizing significant patterns. Irregularities in IoT networks frequently emerge within the context of broader patterns or trends. LSTM effectively captures contextual information from prior observations, which is essential for distinguishing between normal and abnormal behaviors. LSTM networks represent a specific architecture within the realm of RNNs, designed for the purpose of modeling sequences and time-series data. LSTM networks have demonstrated promising results across various applications, such as time-series forecasting, voice recognition, intrusion detection in the IoT, and

natural language processing [11]. The sequential characteristics of IoT data render LSTM a suitable option, as it adeptly captures relationships and patterns over time. The ability of LSTM to analyze sequences of sensor readings or network traffic data could be beneficial for intrusion detection systems, as it allows for the recognition of unusual patterns indicative of potential intrusions. LSTM networks were designed to address the vanishing gradient problem commonly encountered in standard RNNs [12]. This allows LSTM networks to proficiently gather and represent long-term dependencies in sequential data. In the realm of IoT intrusion detection, it is essential to consider both immediate patterns and extended behaviours that could indicate sophisticated attacks. The LSTM model's ability to retain information across extended sequences renders it exceptionally effective in capturing these interdependencies. Additionally, LSTMs possess memory cells capable of retaining data over extended periods, enabling them to remember past events and leverage that information for generating predictions. This is particularly beneficial for identifying intrusions in the IoT, as differentiating between typical and harmful behavior necessitates an analysis of their temporal context.

Enhancing hyper-parameters for deep learning architectures tailored to intrusion detection systems enables the system to proactively safeguard against unauthorized access [13]. The development of these models involved thorough mathematical analysis, which guarantees the conceptual integrity of the system in addressing security threats. Healthcare institutions need to implement strong security measures to ensure that IoMT devices function as intended and are properly configured and deployed. The safety of patients could be compromised if cybercriminals gain access to IoMT devices and overwhelm them with traffic, leading to potential failures or inaccessibility. Utilizing advanced optimization techniques with deep learning models for hyper-parameter tuning enhances resilience to intrusions and bolsters the overall integrity of healthcare systems.

This study examines the limitations associated with slower convergence and the challenges of hyper-parameter adjustments in LSTM. Considering this, the hyper-parameters of LSTM are optimized through a swarm-inspired MAFA method. This study examines the core swarm-based optimization methods, including Particle Swarm Optimization (PSO) and Firefly Algorithm (FA). The main limitation of the swarm intelligence optimization method is its vulnerability to premature convergence and its inadequate ability for local optimization. PSO presents certain drawbacks, including the tendency for early convergence, increased memory demands for updating velocity, and the potential for suboptimal solutions. In a similar manner, within the core framework of FA, a firefly primarily adjusts its position in response to the attraction exerted by nearby fluorescent fireflies. The absence of randomness can lead the entire search space to settle at a local optimum after several iterations. The paper introduces MAFA as a solution to the limitations of basic swarm-based optimization, implementing a fitness diversity adaptation to maintain population diversity and achieve a balance between exploration and exploitation. The methods for adapting fitness diversity assess fitness diversity to gauge population diversity. Alternatively, these techniques may be suggested to create a balance between exploitation and exploration during the search process.

2. ITERATURE REVIEW

Deep learning techniques, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have shown remarkable performance in detecting cyber threats and anomalies in diverse domains, including power systems. CNNs are well-suited for image-based cyber security tasks, such as analyzing network traffic visualizations or satellite imagery of power grid infrastructure. RNNs, on the other hand, are effective in capturing temporal dependencies in sequential data, making them suitable for analyzing time-series data from power system sensors and control devices [21], [22]. Recent studies have demonstrated the effectiveness of deep learning models in detecting cyber-attacks, such as intrusions, data exfiltration, and malware propagation, in power system data streams. By leveraging large-scale labelled datasets and advanced neural network architectures, deep learning models can learn complex patterns indicative of cyber threats with high accuracy and generalization capability [23], [24].

The Internet of Things significantly contributes to the advancement of intelligent systems such as smart cities, homes, and factories; however, its extensive reach and ubiquity present notable security challenges. IoT devices, frequently operating in unmonitored settings and linked wirelessly, are vulnerable to unauthorized access and eavesdropping because of their constrained resources. This vulnerability highlights the

necessity for both diagnostic and preventive security measures, particularly emphasizing the importance of decentralized defense systems. Intrusion detection systems utilizing machine learning and deep learning provide robust security solutions for the Internet of Things, with continuous exploration into advanced development methodologies.

Devendiran et al. [14] introduced an innovative method aimed at enhancing data security through the implementation of a deep learning-based network intrusion detection model. The methodology includes conducting preliminary data cleaning and implementing M-squared normalization, subsequently balancing the dataset through Extended Synthetic Sampling. Feature extraction is achieved through the application of kernel-assisted principal component analysis (K-PCA). Subsequently, the most suitable features are chosen using the Chaotic Honey Badger optimization method. The classification of the attacks employs Gated Attention Dual LSTM (Dugat-LSTM), achieving remarkable accuracy rates of 99.65% and 98.76% on the NSL-KDD and TON-IoT datasets. Wang et al. [15] presented BT-TPF, an IoT intrusion detection model that employs knowledge distillation and is tailored for IoT applications with limited computational resources. The BT-TPF method utilizes a Siamese network to minimize data dimensionality and integrates a Vision Transformer as a guiding framework for developing a Poolformer model. The BT-TPF model achieves an impressive accuracy exceeding 99% on the CIC-IDS2017 and TON_IoT datasets, all while significantly reducing the parameter count.

Managing extensive datasets presents considerable difficulties, requiring significant computational power and leading to prolonged processing durations. To tackle this issue, Sundaram et al. [16] developed efficient intrusion detection systems by employing a hybrid feature selection method that combines information gain with recursive feature elimination (RFE). Following this, a cascaded-LSTM architecture is utilized to improve the accuracy of attack classification. The method under consideration demonstrated binary classification accuracies of 98.96% on the NSL-KDD dataset and 99.30% on the UNSW-NB15 dataset. Utilizing the UNSW-NB15 dataset sourced from Kaggle, Louai A. Maghrabi [17] created an automated NID framework by training the RF model. The experimental results indicate a recall of 90.14%, precision of 90.14%, and an F1 score of 90.14%. These findings demonstrate that the proposed model surpasses the traditional method in accuracy by 7.34%. Furthermore, a balanced class dataset attains an impressive accuracy of 98.83% through the application of random resampling techniques to create synthetic data for minority assaults.

Shakya et al. [18] introduced the Innovative Integrated Reinforcement Learning (RL)-based Advanced DL Algorithm (IRADA), which was specifically designed for the detection of intrusions in Wireless Sensor Networks (WSNs). IRADA demonstrates outstanding effectiveness in intrusion detection through the integration of deep learning and reinforcement learning. The results indicate an accuracy of 99.50%, specificity of 99.94%, sensitivity of 99.48%, F1 score of 98.26%, Kappa statistics of 99.42%, and an area under the curve of 99.38%. Furthermore, the evaluation of IRADA's resilience against adverse attacks confirms its effectiveness in practical security settings. Azimjonov et al. [19] explored constraints by presenting an effective and precise intrusion detection system that utilizes a stochastic gradient descent classifier (SGDC) alongside four feature-selection algorithms grounded in a ridge regressor. In order to enhance the precision of the IDS while minimizing computational expenses, the hyper-parameters of the SGDC method and the ridge regressor model underwent optimization. After examining three network traffic datasets (BotIoT-2018, N-BaIoT-2021, and KDD-CUP-1999), it is evident that the proposed methods highlight a substantial requirement for lightweight intrusion detection systems on IoT devices with limited resources. The assessment revealed an average accuracy of 92.69% along with a significant reduction in the number of features, averaging a decrease of 79.93%. Ahmad et al. [20] introduced a streamlined mini-batch federated learning (FL) approach aimed at identifying vulnerabilities in IoT networks, all while ensuring user privacy is preserved. This method is distinguished by its exceptional computational efficiency and its capacity to minimize the necessary number of federation rounds for detection. The experimental results on standard IoT datasets demonstrate an impressive accuracy of 98.85% in attack detection, accompanied by a minimal false alarm rate of 0.09%. This outcome has been accomplished through the utilization of minimal processing resources.

An in-depth examination of the current literature reveals significant gaps in studies concerning intrusion detection systems that utilize Internet of

Things data. Many earlier investigations concentrate on intrusion detection within traditional IoT datasets, which feature a restricted variety of attack types. The proposed system MAFA-LSTM distinguishes itself from traditional approaches by focusing on the recent TON-IoT dataset, which includes sophisticated attack categories. A highly sensitive IDS generates false alerts, despite the current DL model demonstrating a significant level of accuracy. The interruption of seamless connectivity among IoT devices caused by erroneous positive predictions results in the obstruction of network traffic. Furthermore, it influences the standard of service provided. A significant gap in the existing literature is the insufficient focus on the model's usability, while there is an overemphasis on its correctness. Recent publications have concentrated on the training and optimization of deep learning models to improve the effectiveness of intrusion detection systems. Current trends in the IoT environment emphasize the development of advanced network designs, the integration of various optimization techniques, and the implementation of more efficient feature extraction for intrusion detection systems.

3. PROPOSED METHOD

This study employs MAFA to determine the ideal parameter values, specifically focusing on optimizing. During the MAFA implementation, a combination of local search using perturbation operators and FA is employed to mitigate the risk of premature convergence.

The iterations continue until they meet the stopping condition, which may be determined by either a predetermined number of generations or the lack of additional improvements. Refer to Figure 2 for the fundamental cellular architecture of the proposed LSTM approach. Among the five hyper parameters optimized in this suggested model, emerges as a parameter that substantially influences accuracy as the number of thick layers grows. The primary aim of the proposed MAFA-based methodology is to ascertain optimal values for all assessed LSTM parameters facilitating the detection of malicious traffic in an IoT environment.

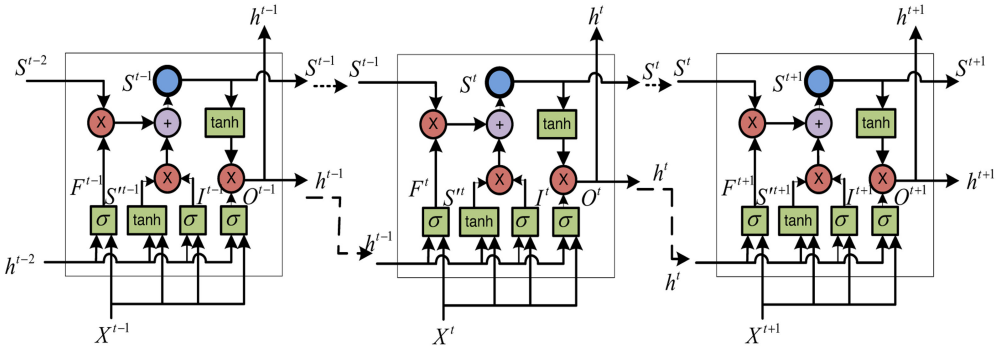

Figure 2. Overall structure of the LSTM network

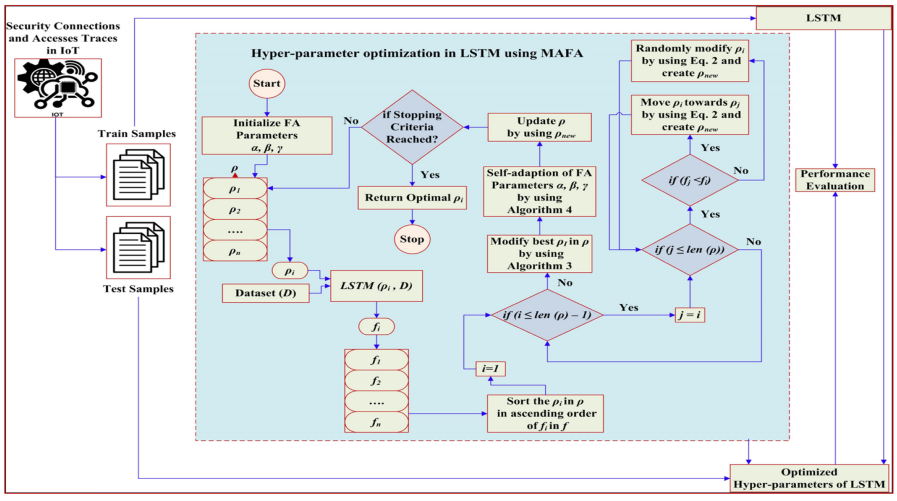

Figure 3. The standard flow architecture of the proposed MAFA-LSTM framework

4. RESULTS AND DISCUSSIONS

This study has been carried out on GPU servers provided by Google Colab, utilizing the TensorFlow and Keras frameworks within a Python notebook. The hardware configuration utilized in this experiment included an Intel Core i9 processor functioning at a frequency of 2.20 GHz, 32 GB of RAM, a Windows 11 operating system (64-bit), and an NVIDIA GeForce GTX 1050 graphics processing unit. Furthermore, the Imblearn and Pandas frameworks have been integrated into the Python library to enhance data analysis capabilities. Data visualization has been accomplished using Matplotlib and Mlxtend, with Sklearn being the chosen framework for data analysis. The Keras library provides functions for deep learning, whereas TensorFlow serves as a versatile and free framework for various deep training tasks.

This study assesses the effectiveness of a new MAFA-based LSTM model utilizing an IoT dataset. This experiment involves a comparison of several advanced techniques, such as NB, DT, RF, LR, ELM, LSTM, PSO algorithm with LSTM, FA-LSTM, and MAFA-LSTM, to evaluate their outcomes. Figure 4 depicts the evolution of fitness over generations for the MAFA-LSTM, FA-LSTM, and PSO-LSTM models. The red line clearly indicates a steady improvement in fitness for MAFA-LSTM in comparison to FA-LSTM. The MAFA-LSTM fitness stays consistent between the 33rd and 40th generations, followed by a significant increase. Figure 5 presents a detailed accuracy analysis, contrasting the proposed method with the different approaches examined. Figures 6, 7, and 8 illustrate the movement of the attractiveness parameter. The findings distinctly illustrate variability in both average and optimal performance across various metrics among all models. The proposed MAFA-LSTM demonstrates exceptional performance, achieving an accuracy of 99.99% and remarkable evaluation metrics, all at 0.99. Next in line is FA-LSTM, achieving an impressive accuracy of 99.96%. Conversely, alternative approaches like PSO-LSTM, LSTM, ELM, RF, LR, DT, and NB yield accuracies of 99.11%, 98.02%, 79.15%, 64.55%, 75.23%, 77.12%, and 64.03% respectively. Ensemble-based methods consistently demonstrate superior performance compared to ML-based approaches in the realm of gesture recognition. It is important to note that the NB method demonstrates lower accuracy compared to LR, DT, and RF, which could be due to its less precise classification of IoT attacks. The proposed method shows effective results in identifying these attacks, highlighting the important role of hyper-parameter tuning in LSTM.

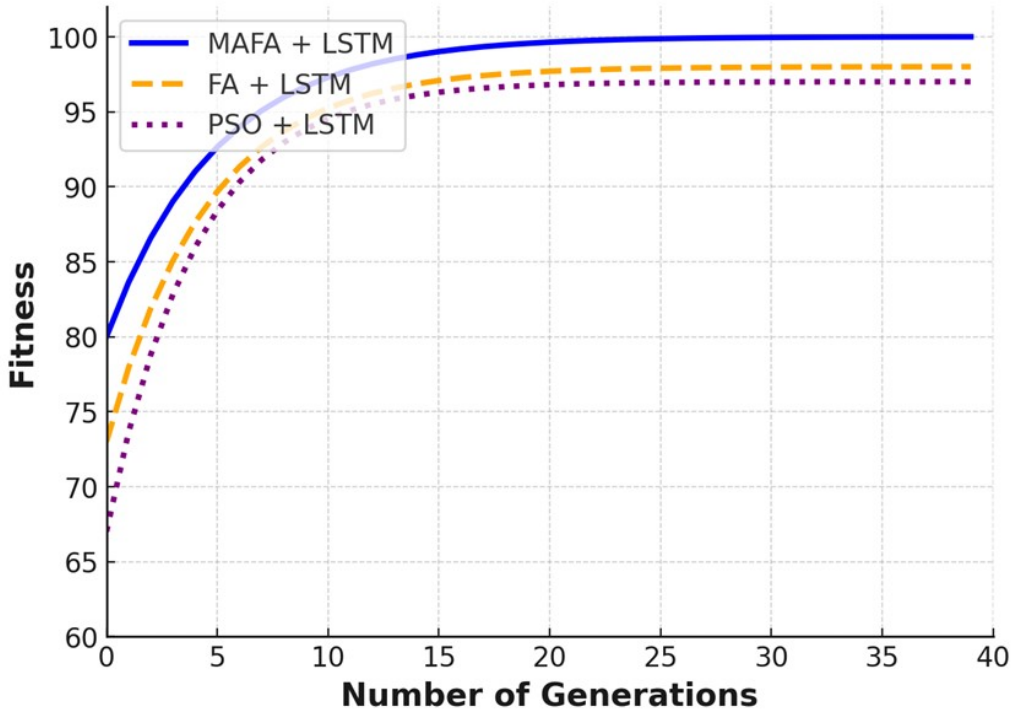

Figure 4. Evolution of fitness across multiple generations

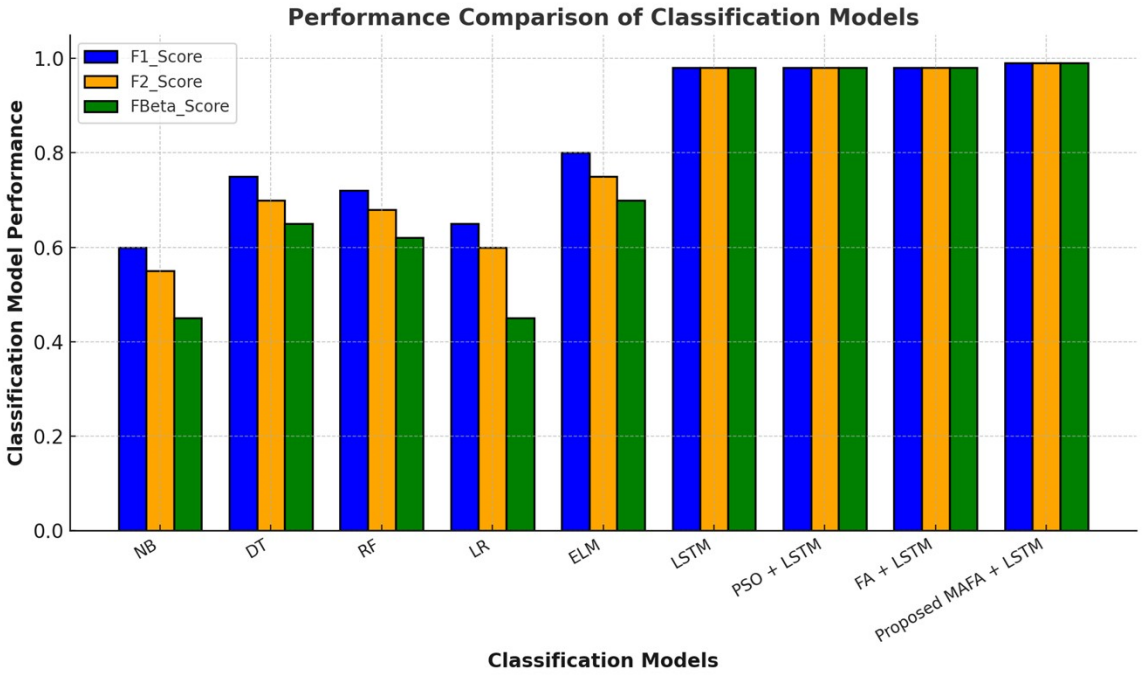

Figure 5. Evaluation of performance

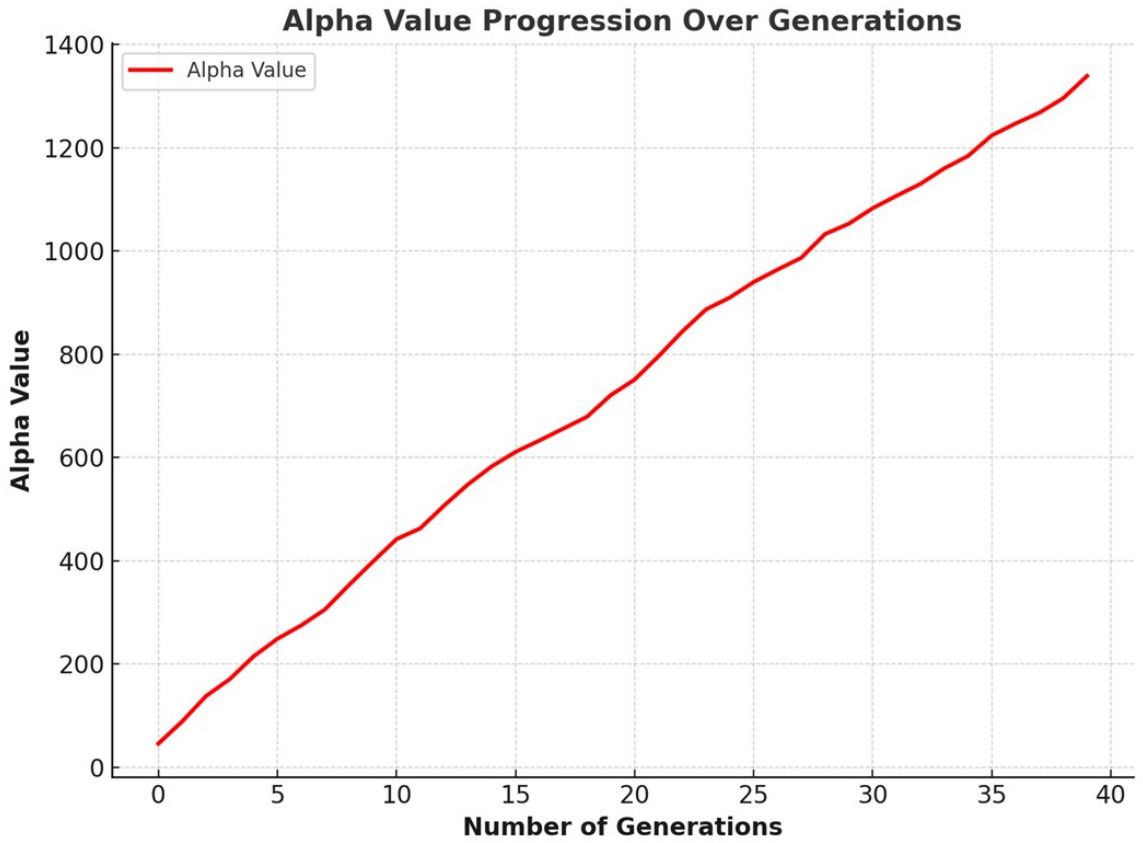

Figure 6. Alpha parameter

Journal of Theoretical and Applied Information Technology
15st June 2026. Vol.104. No.11

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

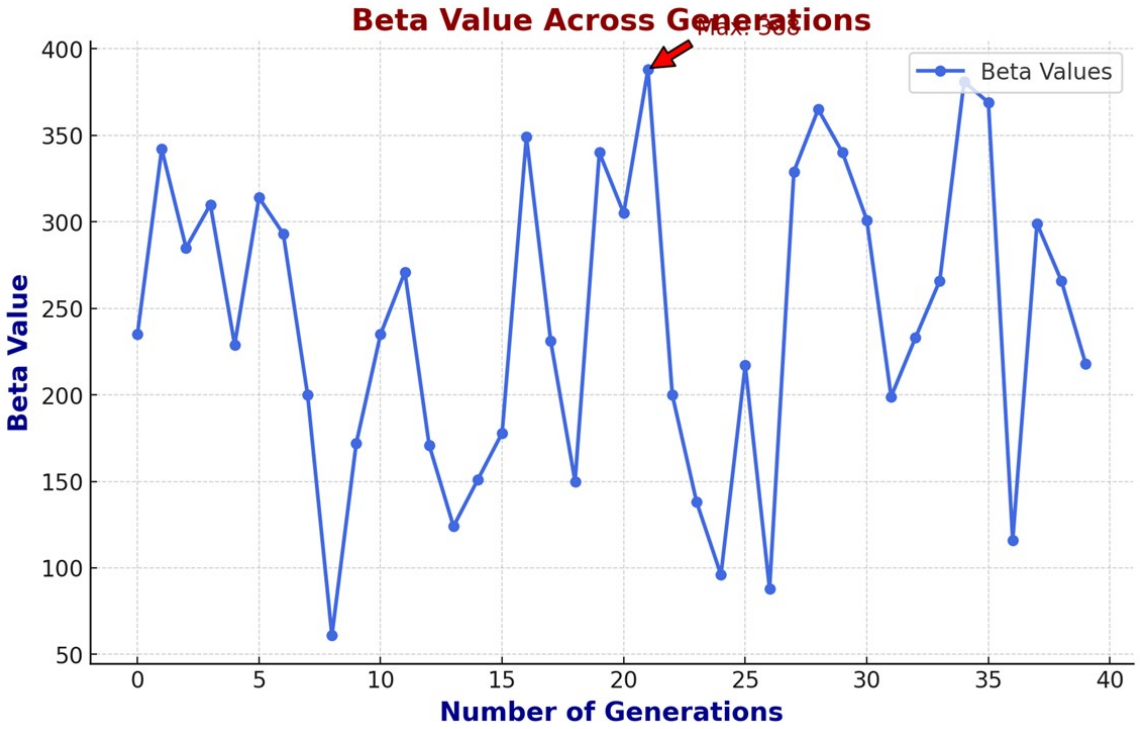

Figure 7. Beta Parameter

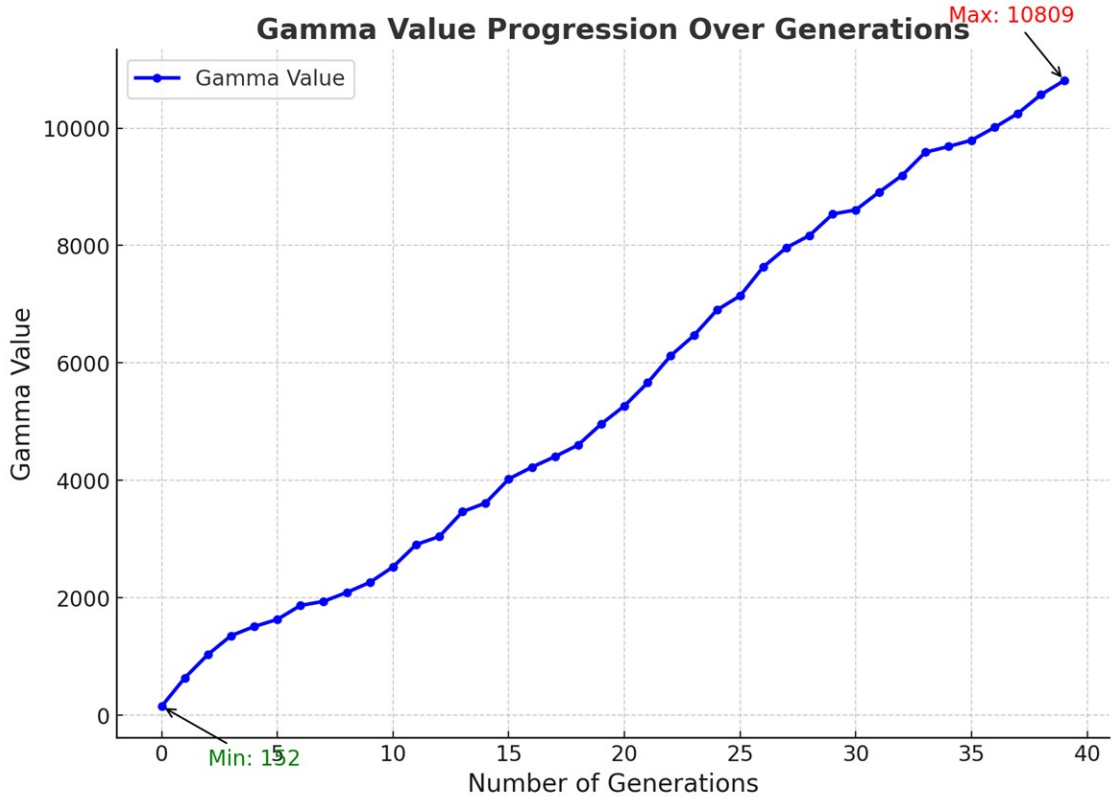

Figure 8. Gamma parameter

To illustrate the efficacy of the proposed MAFA-LSTM algorithm in detecting abnormal behaviors within the IoT environment, the simulation results are juxtaposed with findings from other research that has explored prediction techniques utilizing various IoT datasets, including CIC-IDS2017, N-Balot, WSN-DS, InSDN dataset, TON-IoT, and BoTNet datasets.

5. CONCLUSION

With the recent increase in demand for IoT networks, safeguarding the communication profiles of IoT devices has become increasingly crucial. A number of experts are concentrating on this domain to create innovative techniques for accurately identifying irregularities in intricate IoT systems, aiming to safeguard the IoT from a diverse range of attacks. Although many machine learning techniques have proven effective in identifying outliers within a static context, these approaches may struggle to deliver precise predictions for unforeseen attacks. This study involves the design and testing of various classifier algorithms aimed at developing an intrusion detection system tailored for the IoT environment. The PSO, FA, and MAFA methods have been utilized to identify the optimal parameters appropriate for the proposed LSTM classification model. The application of hyper-parameter tuning will affect the effectiveness of the proposed model for classification. Furthermore, a variety of machine learning algorithms, such as logistic regression, naive Bayes, random forest, decision trees, extreme learning machines, and long short-term memory networks, are assessed to confirm the efficacy of the proposed approach. PSO-LSTM, FA-LSTM, and particularly MAFA-LSTM stand out as the most effective methods, as they yield results that enable the detection of anomalies with remarkable precision. The proposed MAFA-LSTM model demonstrates an impressive accuracy rate of 99.99%, along with precision and recall values of 0.9999. The results indicate remarkable F1 and F2 scores of 0.9999, along with an exceptional ROC-AUC score of 1.0. In the near future, initiatives will focus on engaging with a dataset that features a greater number of cases, along with increased complexity and comprehensive inclusion criteria.

REFERENCES:

[1]. Sharma N, Shamkuwar M, Singh I. The history, present and future with IoT. Internet of things and big data analytics for smart generation 2019:27–51. https:// doi.org/10.1007/978-3-030-04203-5_3.

[2]. Arasteh H, et al. Iot-based smart cities: a survey. In: 2016 IEEE 16th international conference on environment and electrical engineering (EEEIC). IEEE; 2016. https://doi.org/10.1109/EEEIC.2016.7555867.

[3]. Stellios I, et al. A survey of iot-enabled cyberattacks: assessing attack paths to critical infrastructures and services. IEEE Commun Surv Tutor 2018;20(4): 3453–95. https://doi.org/10.1109/COMST.2018.285556

[4]. Baddu Naik Bhukya, V. Venkataiah, S. Mani.Kuchibhatla, S. Koteswari, R V S Lakshmi Kumari, and Yallapragada Ravi Raju, "Integrating the Internet of Things to Protect Electric Vehicle Control Systems from Cyber Attacks," IAENG International Journal of Applied Mathematics, vol. 54, no. 3, pp433-440, 2024.

[5]. Mangla M, et al. A proposed framework to achieve CIA in IoT networks. In: International Conference on Artificial Intelligence and Sustainable Engineering: Select Proceedings of AISE 20202. Springer Singapore; 2022. https://doi.org/10.1007/978-981-16-8546-0_3.

[6]. Mohindru G, Mondal K, Banka H. Different hybrid machine intelligence techniques for handling IoT-based imbalanced data. CAAI Transact Intell Technol 2021; 6(4):405–16. https://doi.org/10.1049/cit2.12032.

[7]. B. N. Bhukya, S. M. Kuchibhatla, N. K. Bhagavatham, T. L. Narayana, M. R. Chunduru, and B. K. Madhavi, “Implementation of meta-heuristic and deep learning algorithms for power system cybersecurity,” Bulletin of Electrical Engineering and Informatics, vol. 15, no. 1, pp. 648–656, Feb. 2026, doi: 10.11591/eei. v15i1. 8569.

[8]. Reddy DKK, Nayak J, Behera HS. A hybrid semi-supervised learning with nature-inspired optimization for intrusion detection system in iot environment. In: International Conference on Computational Intelligence in Pattern Recognition. Springer Nature Singapore; 2022. https://doi.org/10.1007/978-981-19-3089-8_ 55.

[9]. Li Z, et al. A survey of convolutional neural networks: analysis, applications, and prospects. IEEE Transact Neur Netw Learn Syst 2021;33(12):6999–7019. https://doi.org/10.1109/TNNLS.2021.3084827.

[10]. B. Baddu Naik, M. Ravindra, S. M. Rao, S. Kilaru, M. Brahmaiah, B. Manasa, and M. V., “Cyberattack prevention and detection in smart power systems using deep learning,” Journal of Theoretical and Applied Information

Technology, vol. 103, no. 9, pp. 3934–3944, May 2025.

[11]. Cheng Y, Xu Y, Zhong H, Liu Y. Leveraging semisupervised hierarchical stacking temporal convolutional network for anomaly detection in IoT communication. IEEE IoT J Jan. 2021:144–55. https://doi.org/10.1109/JIOT.2020.3000771.

[12]. Sherstinsky A. Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network. Physica D: Nonlin Phenom 2020; 404:132306. https://doi.org/10.1016/j.physd.2019.132306.

[13]. B. N. Bhukya, S. M. Kuchibhatla, N. K. Bhagavatham, T. L. Narayana, M. R. Chunduru, and B. K. Madhavi, "Implementation of meta-heuristic and deep learning algorithms for power system cybersecurity," Bulletin of Electrical Engineering and Informatics, vol. 15, no. 1, pp. 648–656, Feb. 2026, doi: 10.11591/eei. v15i1.8569.

[14]. Devendiran R, Turukmane AV. Dugat-LSTM: deep learning based network intrusion detection system using chaotic optimization strategy. Exp Syst Applic 2024; 245:123027. https://doi.org/10.1016/j.eswa.2023.123027.

[15]. K. Cherukupalli, B. N. Bhukya, and P. R. Chinda, "Enhancing power system security with a hybrid SATS algorithm for optimal power flow," Journal of Theoretical and Applied Information Technology, vol. 103, no. 6, pp. 2175–2183, Mar. 2025.

[16]. Sundaram K, et al. A novel hybrid feature selection with cascaded LSTM: enhancing security in IoT networks. Wirel Commun Mob Comput 2024 2024. https:// doi.org/10.1155/2024/5522431.

[17]. Maghrabi LA. Automated network intrusion detection for internet of things security enhancements. IEEE Access 2024. https://doi.org/10.1109/ ACCESS.2024.3369237.

[18]. Shakya V, Choudhary J, Singh DP. IRADA: integrated reinforcement learning and deep learning algorithm for attack detection in wireless sensor networks. Multim Tool Applic 2024:1–20. https://doi.org/10.1007/s11042-024-18289-7.

[19]. S. R. Bondalapati, S. Narkedamilli, R. V. S. L. Kumari, K. V. S. Reddy, N. Chippada, J. M. R. Danda, and P. S. Subhashini, "Smart vehicle cybersecurity: Implementing an autonomous and adaptive intrusion response system," ASEAN Engineering Journal, vol. 15, no. 4, pp. 221–228, Nov. 2025, doi: 10.11113/aej. V15.24631.

[20]. B. N. Bhukya and K. Cherukupalli, "A novel hybrid optimization approach for solving security-constrained optimal power flow problems," IAENG International Journal of Computer Science, vol. 52, no. 9, pp. 1–10, 2025.