Enhancing IoT Network Security: ML and Blockchain for Intrusion Detection

N. Sunanda[1], K. Shailaja[2], Prabhakar Kandukuri[3],
Krishnamoorthy[4], Vuda Sreenivasa Rao[5], Sanjiv Rao Godla[6]
Assistant Professor, Department of CSE-(CyS,DS) and AI&DS ,VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India[1]
Associate Professor, Department of CSE, Vasavi College of Engineering, Hyderabad, India[2]
Professor, Department of Artificial Intelligence and Machine Learning,
Chaitanya Bharathi Institute of Technology - Hyderabad, India[3]
Associate Professor, Department of CSE, Panimalar Engineering College, Chennai, India[4]
Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India[5]
Professor, Department of CSE (Artificial Intelligence & Machine Learning), Aditya College of Engineering & Technology - Surampalem, Andhra Pradesh, India[6]

***Abstract*—Given the proliferation of connected devices and the evolving threat landscape, intrusion detection plays a pivotal role in safeguarding IoT networks. However, traditional methodologies struggle to adapt to the dynamic and diverse settings of IoT environments. To address these challenges, this study proposes an innovative framework that leverages machine learning, specifically Red Fox Optimization (RFO) for feature selection, and Attention-based Bidirectional Long Short-Term Memory (Bi-LSTM). Additionally, the integration of blockchain technology is explored to provide immutable and tamper-proof logs of detected intrusions, bolstering the overall security of the system. Previous research has highlighted the limitations of conventional intrusion detection techniques in IoT networks, particularly in accommodating diverse data sources and rapidly evolving attack strategies. The attention mechanism enables the model to concentrate on pertinent features, enhancing the accuracy and efficiency of anomaly and malicious activity detection in IoT traffic. Furthermore, the utilization of RFO for feature selection aims to reduce data dimensionality and enhance the scalability of the intrusion detection system. Moreover, the inclusion of blockchain technology enhances security by ensuring the integrity and immutability of intrusion detection logs. The proposed framework is implemented using Python for machine learning tasks and Solidity for blockchain development. Experimental findings demonstrate the efficacy of the approach, achieving a detection accuracy of approximately 98.9% on real-world IoT datasets. These results underscore the significance of the research in advancing IoT security practices. By amalgamating machine learning, optimization techniques, and blockchain technology, this framework provides a robust and scalable solution for intrusion detection in IoT networks, fostering improved efficiency and security in interconnected environments.**

Keywords*—Intrusion detection; IoT networks; machine learning; random forest, red fox optimization; blockchain technology

I. Introduction

The Internet of Things (IoT) represents a transformative innovation in automation and connectivity, comprising a vast network of interconnected devices equipped with actuators, sensors, and computational capabilities [1]. These devices encompass a diverse range, from everyday items like household appliances and wearables to complex industrial machinery and infrastructure components. Central to IoT networks is their autonomous ability to collect, process, and transmit data, eliminating the need for direct human intervention. This autonomy empowers organizations and individuals to leverage data-driven insights and automation across various sectors and industries. For instance, in smart homes, IoT devices facilitate energy monitoring, remote appliance control, and enhanced security via connected surveillance systems [2].

Wearable sensors and medical gadgets help with early health issue diagnosis, individualized treatment strategies, and remote patient monitoring in the healthcare industry. In transportation, IoT technologies optimize logistics, improve traffic management, and enhance passenger safety through intelligent vehicle systems and infrastructure. Moreover, IoT networks extend their reach into diverse sectors such as agriculture, where precision farming techniques leverage sensor data to optimize irrigation, monitor soil conditions, and maximize crop yields[3]. In industrial settings, IoT-enabled machinery and production systems enable predictive maintenance, real-time monitoring of equipment health, and automation of manufacturing processes, leading to increased efficiency and reduced downtime. The overarching goal of IoT networks is to enhance connectivity, efficiency, and convenience while enabling new levels of automation and control across various domains. By seamlessly integrating physical devices with digital technologies, IoT networks pave the way for a more interconnected and intelligent world, where data-driven insights drive decision-making and innovation. However, this proliferation of connected devices

also brings about significant challenges, particularly in terms of security, privacy, and interoperability, which must be addressed to fully realize the potential benefits of the IoT revolution [4].

IoT networks exhibit a high degree of heterogeneity, encompassing a diverse array of devices with varying computational capabilities, communication protocols, and operating systems. From simple sensors to complex smart appliances and industrial machinery, these devices run on different platforms, including embedded systems, Linux-based platforms, and proprietary firmware[5]. This heterogeneity poses challenges for interoperability and standardization. Moreover, IoT networks are highly scalable, capable of supporting deployments ranging from small-scale implementations to massive infrastructures comprising millions of interconnected devices. This scalability leads to complex network topologies and management challenges. Connectivity serves as a cornerstone for IoT networks, with devices employing a range of wired and wireless communication technologies. The selection of connectivity technology is influenced by factors such as range, power consumption, and deployment environment. Additionally, IoT networks generate a wide array of data types, including sensor readings, images, audio, and video streams, presenting challenges for data processing and analysis. Effectively managing this data diversity is essential for deriving meaningful insights while maintaining scalability, efficiency, and data privacy [6].

IoT networks are susceptible to a myriad of security vulnerabilities, posing significant challenges to their integrity and reliability. Weak authentication and authorization mechanisms represent a prevalent threat, as many IoT devices are shipped with default or easily guessable credentials, providing malicious actors with unauthorized access and control over these devices [7]. Furthermore, insecure communication practices exacerbate the risk, as IoT devices often transmit data over unencrypted channels or employ weak encryption protocols, leaving sensitive information vulnerable to eavesdropping and interception by malicious entities. Compounding these issues is the lack of timely security updates from manufacturers, leaving devices exposed to known vulnerabilities and exploits. Physical vulnerabilities also pose a substantial risk to IoT networks, as attackers can exploit physical access to tamper with hardware components, extract sensitive data, or implant malicious firmware, compromising the integrity and functionality of these devices [8].

Additionally, IoT devices are susceptible to being co-opted into botnets and used to launch distributed denial-of-service (DoS) attacks against targeted services or networks, leading to disruptions and downtime. Moreover, the vast amounts of personal and sensitive data collected and transmitted by IoT devices raise significant privacy concerns, including unauthorized access, data breaches, and misuse of information. Supply chain risks further exacerbate the security landscape, as the global supply chain for IoT devices is often complex and opaque, making it challenging to verify the integrity and authenticity of hardware components and software firmware [9]. Lastly, interoperability issues between IoT devices and protocols introduce additional vulnerabilities, enabling attackers to exploit weaknesses in communication interfaces and protocols, potentially compromising the entire network. A comprehensive strategy that includes strong authentication procedures, encryption methods, regular security upgrades, physical security measures, and privacy-enhancing technology is needed to address these issues. In addition, stakeholders need to work together to create industry-wide guidelines and recommendations for protecting IoT networks and devices, minimizing risks, and guaranteeing the dependability and trustworthiness of the IoT ecosystems [10].

Intrusion detection in IoT networks is hindered by the dynamic and heterogeneous nature of these environments, along with the continuously evolving threat landscape. Traditional methods struggle to adapt to the diverse array of devices, communication protocols, and data formats present in IoT networks, leading to limited coverage and effectiveness. Scalability poses another challenge, as the sheer volume of interconnected devices generates large amounts of data that traditional systems may struggle to process in real-time. Resource constraints on IoT devices further complicate matters, making it difficult to deploy traditional intrusion detection solutions. Furthermore, newer or undiscovered threats could not be detected by conventional techniques, calling for more sophisticated detection capabilities. Moreover, worries about data privacy and integrity continue since centralized systems have the potential to expose vulnerabilities or corrupt critical data. Innovative solutions that are suited to the special features of internet of things networks are needed to tackle these issues. These solutions must be scalable, resource-efficient, capable of robust detection, and equipped with improved security mechanisms to efficiently reduce hazards [11].

The rapid expansion of Internet of Things (IoT) networks has underscored the critical need for a robust and scalable intrusion detection framework capable of effectively mitigating security threats. Traditional intrusion detection systems (IDS) often struggle to adapt to the dynamic and heterogeneous nature of IoT environments, necessitating innovative solutions. Our research is motivated by the imperative to develop such a framework, leveraging advanced machine learning techniques like Attention-based Bidirectional Long Short-Term Memory (BiLSTM) networks for real-time threat detection. Additionally, the integration of Red Fox Optimization (RFO) enhances the efficiency of feature selection, enabling more accurate identification of relevant data amidst the complexities of IoT networks. Furthermore, the incorporation of blockchain technology ensures the integrity and trustworthiness of intrusion detection data, facilitating transparent incident response and forensic analysis. By synergizing these technologies, our framework offers a comprehensive defense mechanism against evolving threats, safeguarding critical assets and bolstering the security posture of IoT ecosystems. The key contribution of the research is stated as follows:

- The research presents a pioneering framework that combines machine learning techniques, such as Attention-based BiLSTM networks, with Red Fox

Optimization for feature selection, providing a novel approach to intrusion detection in IoT networks.

- By leveraging advanced machine learning algorithms, our framework achieves a significantly higher detection accuracy of approximately 98%, surpassing traditional intrusion detection systems and effectively mitigating security threats in IoT environments.
- The integration of Red Fox Optimization streamlines feature selection, enhancing the scalability and efficiency of our framework in handling the dynamic and heterogeneous nature of IoT data streams, thus ensuring robust performance even in large-scale IoT deployments.
- Incorporating blockchain technology ensures the integrity and tamper-resistance of intrusion detection data, providing transparent incident response and forensic analysis capabilities, thereby enhancing the overall security and trustworthiness of IoT networks.

The paper begins with an introduction to the research topic in Section I, followed by a comprehensive review of related literature in Section II. The methodology in Section IV outlines the proposed framework's design and implementation, with Section V covering experimental evaluation, results analysis, and discussion on the framework's effectiveness. Finally, Section VI concludes the paper.

II. Related Works

Strong security mechanisms inside IoT networks are vital, as evidenced by the increasing ubiquity of Internet of Things (IoT) technologies. But in Internet of Things contexts, conventional intrusion detection systems face severe restrictions because of limited resources and the intrinsic complexity of the network. Liang et al. [12] research aims to tackle these issues by developing, putting into practice, and assessing a novel intrusion detection system. This system makes use of deep learning algorithms, blockchain technology, and multi-agent systems as part of a hybrid placement strategy. The data collecting, management, analysis, and reaction components of the system are organised into separate modules. The National Security Lab's NSL-KDD dataset was used for experimental verification, which demonstrates how well deep learning algorithms detect assaults, especially at the IoT network's transport layer. Notwithstanding the encouraging outcomes, the study admits significant limitations, such as the requirement for additional improvement and optimisation of the suggested system in order to guarantee its scalability and suitability for use in a variety of IoT scenarios.

Alkadi et al. [13] paper presents a novel approach to collaborative intrusion detection for safeguarding IoT and cloud networks, leveraging the capabilities of deep blockchain technology. By integrating blockchain into intrusion detection systems, the proposed framework aims to enhance the security posture of interconnected environments through collaborative threat intelligence sharing and consensus-driven decision-making processes. Through the utilization of machine learning algorithms and distributed ledger technology, the framework enables real-time detection and response to emerging threats across diverse network landscapes. Experimental results demonstrate the efficacy of the framework in detecting intrusions and mitigating security risks in various network scenarios. However, the adoption of deep blockchain technology introduces challenges related to scalability, latency, and resource consumption. The computational overhead associated with maintaining a distributed ledger across multiple nodes may impact the real-time responsiveness of the intrusion detection system. Furthermore, ensuring consensus among distributed nodes in a timely manner can pose synchronization and coordination challenges, potentially affecting the system's overall efficiency and effectiveness in rapidly evolving threat landscapes. Addressing these scalability and performance limitations is essential to realize the full potential of the proposed framework in large-scale IoT and cloud networks.

The necessity for strong security measures to protect Internet-of-things (IoT) environments from potential threats has been highlighted by the growth of IoT devices. In order to protect computer networks, including the Internet of Things, from many types of security breaches, intrusion detection systems, or IDSs, are essential. The utilisation of collaborative intrusion detection systems or networks, also known as CIDSs or CIDNs, has shown promise in improving detection performance through the sharing of vital information across IDS nodes, including signatures and alarms. Nevertheless, because collaborative networks are distributed, they are vulnerable to insider assaults, in which rogue nodes spread fake signatures, jeopardising the accuracy and effectiveness of intrusion detection systems. Using blockchain technology presents a viable way to safely validate shared signatures. In this regard, the research of Li et al. (Li et al. 2019) presents CBSigIDS, an innovative framework for blockchain-based collaborative signature-based IDSs intended to create and gradually update a trusted signature database in collaborative IoT contexts. With no need for a reliable middleman, CBSigIDS provides a verified method in distributed architectures. Although CBSigIDS shows promise in strengthening the efficiency and robustness of signature-based IDSs, a significant disadvantage is the possible overhead related to blockchain activities, which calls for additional optimisation to guarantee scalability and efficacy in practical deployments.

Issues with privacy, security, and single points of failure in centralised storage structures still exist as the Internet of Things (IoT) gains pace, especially in crucial applications. By providing decentralised and secure data management, blockchain technology has emerged as a viable answer to these problems. There is a lot of potential for improving social and economic advantages when blockchain is integrated with IoT. But as the 2017 attack on a pool of miners has shown, blockchain-enabled Internet of Things (IoT) networks are vulnerable to Distributed Denial of Service (DDoS) attacks, underscoring the necessity of strong security protocols. Furthermore, for efficient analysis and decision-making, these applications' enormous data generation demands the use of sophisticated analytical tools like machine learning (ML). In order to address these issues, a unique solution is presented in

the paper by Kumar et al. [14]. This paper presents a distributed Intrusion Detection System (IDS) intended to detect distributed denial of service (DDoS) assaults targeting mining pools within Internet of Things networks, using fog computing and blockchain technology. Using Random Forest (RF) and an optimised gradient tree boosting system (XGBoost), both trained on dispersed fog nodes, the efficacy of the suggested IDS is evaluated. The BoT-IoT dataset, which covers recent assaults seen in IoT networks with blockchain support, is used in the evaluation. The possible costs and difficulties of implementing a distributed IDS employing fog computing in practical settings might be a drawback of the recommended strategy, necessitating more study and optimisation for efficiency and scalability. However, the outcomes demonstrate that Random Forest outperforms XGBoost in multi-attack recognition and binary attack detection.

Protecting industrial IoT (IIoT) networks from security threats is crucial as these networks grow to be essential parts of vital infrastructure. Numerous strategies utilizing Blockchain algorithms and machine learning techniques have been investigated separately to overcome this problem. However, Vargas et al. [15] offer an integrated strategy in this research that integrates these approaches to produce a thorough defense mechanism for networks of Internet of Things devices. The objectives of this mechanism are to identify potential dangers, initiate safe channels for information exchange, and adjust to the processing power of industrial Internet of things settings. The suggested method offers a workable way to identify and stop intrusions in Internet of Things networks and shows effectiveness in accomplishing its goals. Despite its achievements, it's crucial to remember that the suggested integrated strategy can present challenges for management and implementation, necessitating the need for extra funding and knowledge for deployment in actual IIoT scenarios. More investigation is required to ensure scalability and efficiency while minimizing overhead by streamlining and optimizing the integration process.

III. Problem Statement

Despite the notable advancements in intrusion detection systems (IDS) and the integration of blockchain technology and machine learning techniques in securing Internet of Things (IoT) networks, several research gaps persist. Existing studies focus predominantly on individual aspects such as deep learning algorithms, blockchain-based intrusion detection, or collaborative signature-based IDSs. However, there is a scarcity of research that comprehensively addresses the complex security challenges of IoT environments by integrating multiple technologies and methodologies. Furthermore, scalability, efficiency, and practical feasibility remain critical concerns across these studies, indicating the need for further exploration and refinement. Thus, our research aims to bridge this gap by proposing a holistic framework that combines deep learning algorithms, blockchain technology, and collaborative intrusion detection mechanisms to provide robust security solutions for IoT networks. By addressing these multifaceted challenges and evaluating the proposed framework's scalability and effectiveness across diverse IoT scenarios, our research endeavors to contribute towards the development of comprehensive and practical security solutions tailored for IoT environments.

IV. Methodological Integration of ML and Blockchain for IoT Intrusion Detection

The suggested method builds a strong intrusion detection system (IDS) that is suited for the complex architecture of Internet of Things networks by fusing blockchain technology with machine learning. Network traffic, sensor readings, device logs, and other data from IoT devices are first gathered and preprocessed to extract pertinent attributes that are essential for intrusion detection. The framework optimizes feature subsets to increase intrusion detection efficacy and efficiency using the Red Fox Optimization (RFO) approach. Then, real-time anomaly detection is achieved by using Attention (BiLSTM) networks, which take advantage of their capacity to process sequential data streams present in Internet of Things settings. Blockchain technology is easily incorporated to guarantee the immutability and integrity of intrusion detection data. Smart contracts are utilized to provide safe communication and consensus building across dispersed Internet of Things devices, guaranteeing the accuracy and consistency of the data. Benchmark datasets such as the NSL-KDD dataset are used to evaluate the framework's performance in detail across a range of intrusion situations. By employing this technique, researchers want to enhance the efficacy and security of intrusion detection in internet of things networks, as well as tackle the constantly evolving problems associated with IoT setups [16].The suggested technique's architecture is depicted in Fig. 1.

A. Data Collection

The data collection process involves gathering information from IoT devices, drawing upon a diverse array of network traffic, sensor readings, and device logs. In this research, we utilize the NSL-KDD dataset, an open-source resource available on Kaggle [17], to facilitate the collection of comprehensive data for intrusion detection system development. The NSL-KDD dataset offers a rich repository of labeled network traffic data, encompassing various types of attacks and normal behaviors, thereby enabling thorough analysis and evaluation of intrusion detection algorithms. Leveraging this openly accessible dataset ensures transparency and reproducibility in our research methodology, allowing for robust validation and benchmarking of the proposed intrusion detection framework against a standardized dataset. Through meticulous data collection from the NSL-KDD dataset, we aim to capture the diverse range of potential threats and normal activities prevalent in IoT networks, laying the foundation for effective intrusion detection system design and evaluation.

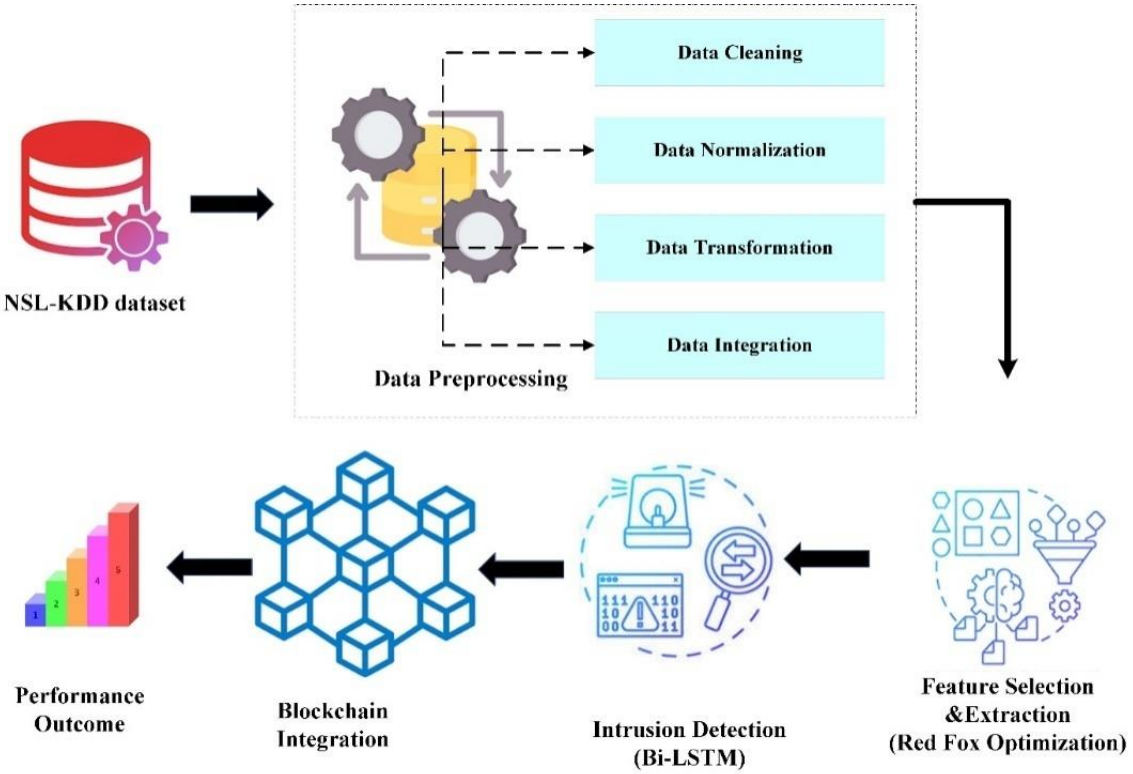

Fig. 1. Proposed integration of ML and blockchain for IoT intrusion detection.

B. Data Preprocessing

Following data collection, the input data undergoes preprocessing to eliminate unwanted noise and address missing data. This involves four key preprocessing approaches:

- Data Cleaning
- Normalization
- Data Transformation
- Data Integration

C. Data Cleaning

In order to improve the quality and dependability of datasets, data cleaning is an essential step in the data preparation pipeline. It involves locating and correcting different kinds of data abnormalities. These anomalies may include corrupted, incorrect, duplicate, or improperly formatted data entries. The primary goal of data cleaning is to ensure that datasets are standardized, accurate, and easily accessible for analysis and query purposes. During the data cleaning process, several tasks are performed to address different types of data issues. Firstly, corrupted or incorrect data entries are identified and either removed or corrected to restore data integrity. Duplicate entries, if present, are identified and eliminated to prevent redundancy and ensure that each observation is unique[18]. Additionally, managing missing values—which can occur for a number of reasons, including incomplete records or mistakes in data collection—is another aspect of data cleansing. When there are missing values in an observation, they can be imputed using statistical techniques or data from other observations can be dropped. Additionally, data cleaning ensures that the dataset complies with the required format and schema by addressing structural flaws that could arise throughout the data transfer process. Thorough data cleaning improves the dataset's dependability and suitability for analysis, allowing analysts and researchers to derive precise conclusions and make defensible choices [19].

D. Normalization

Normalization is a preprocessing step aimed at transforming data from its existing range to a new range. Given the presence of uncertain and incomplete data in the dataset, it becomes essential to address missing or irrelevant data to enhance data quality. The dataset can be integrated and normalized with success using the Min Max normalization approach. By making sure the dataset is scaled correctly, this method makes it possible to anticipate outcomes within the new range and allow for a greater difference in forecasting. Normalization reduces the influence of differences in dataset scales by scaling the dataset so that normalized values lie between 0 and 1. This allows for easier comparison of results from various datasets. This technique involves deducting the minimum value from the variable requiring normalization, resulting in a standardized dataset suitable for analysis and comparison. Min-max scaling, frequently referred to as feature scaling, converts the values of each feature to a range of 0 to 1 [20]. To compute the min-max scaling, use Eq. (1).

$$A_{scaled} = \frac{A - A_{min}}{A_{max} - A_{min}} \quad (1)$$

A is the starting value, $A_{min}$is the smallest value, and $A_{max}$is the largest value in the dataset. This method is helpful when the features are not evenly distributed and have a small range.

E. Data Transformation

Data transformation involves converting the original dataset into a specific format that facilitates faster and more efficient retrieval of strategic insights. Raw datasets can be challenging to comprehend and track, necessitating transformation into a more suitable form before extracting information. This transformation process is crucial for providing easily interpretable patterns, aligning with the strategic objectives of data conversion. Various techniques, such as smoothing, aggregation, and generalization, are employed in data transformation to streamline the dataset. Smoothing techniques are utilized to eliminate noise from the dataset, enhancing data clarity. Data aggregation gathers and presents data in a summarized format, aiding in easier analysis and interpretation. Additionally, data generalization involves converting lower-level or raw data into higher-level data through hierarchical concepts, further enhancing the dataset's organizational structure and usability [21].

F. Data Integration

Data integration is a preprocessing strategy that combines data from several sources into a single data repository to give rich views of the data. These sources could be flat files, databases, or several data cubes. Collaboration between users at all levels is facilitated by data integration, which combines received data with heterogeneous datasets to store consistent data that is client-accessible. A triplet defines the data integration mechanism, which is further explained in Eq. (2).

$$D_1 =< U, V, W > \tag{2}$$

In this context, D_1represents the process of data integration, where U stands for the global schema, V denotes the schema of heterogeneous sources, and W refers to the mappings between queries of the source and global schema [22].

G. Feature Selection

In order to improve the effectiveness and productivity of the intrusion detection process, feature selection is an essential step in the preliminary processing phase of systems for detection. Its goal is to pick the most pertinent characteristics from the pre-processed data. Red Fox Optimisation (RFO) becomes apparent as a potent feature selection method in this scenario. To increase the intrusion detection system's overall performance, RFO works by optimising feature subsets. Finding a subset of characteristics that maximises the discrimination between normal and aberrant network behaviour is the main goal of feature selection using RFO. This will improve the system's capacity to detect intrusions effectively while reducing computing overhead. RFO does this by iteratively assessing and honing potential feature subsets according to pre-established optimisation standards, including performance metrics or classification accuracy. The intrusion detection system may efficiently prioritise and concentrate on the most useful aspects by using RFO for feature selection. This lowers the dimensionality of the data and boosts the overall effectiveness of the detection process. Additionally, RFO has the flexibility and scalability to manage high-dimensional information that are frequently seen in Internet of Things networks [23].

After obtaining the balanced dataset from the previous stage, the optimal features for improving intrusion detection training speed and accuracy are selected using the DRF optimisation technique. Numerous meta-heuristic optimisation strategies are developed to improve network security in standard systems for detection of intrusions. Three newly created models used for network security are Spider Monkey Optimisation, Fruity Optimisation, and Greedy Swarm Optimisation. However, overfitting, which delayed processing, a slower rate of convergence, and complex computational procedures are the main causes of its issues. Generally speaking, some of the most current nature-inspired/bio-inspired optimisation approaches produced is the Dragon Fly Algorithm, Moth Flame Optimisation, and Ant Lion Optimisation, Harris Hawk optimisation (HHO), Flower Pollination Algorithm. These algorithms are commonly used to solve complex optimisation problems in a variety of security applications. The DRF is one of the newest optimisation algorithms and has several advantages over previous techniques. It has a low processing cost, less local optimum, rapid convergence, and guards against algorithm stacking during optimisation. Furthermore, the DRF35 is not specifically utilised in applications for IoT-IDS security. Therefore, the goal of the proposed study is to use this method to dataset feature optimisation based on the best optimum solution. Additionally, this optimisation procedure facilitates a simpler classification method with a higher assault detection rate [23].

The balanced IoT dataset's characteristics may be optimally tuned using this optimization approach. Foxes belong to many Canidae families and are tiny to medium-sized omnivore animals with pointed noses, long, thin legs, thicktails, and slender limbs. The foxes may also be distinguished from each other of their family and from large dogs. A novel meta-heuristic optimization system called the DRF takes its cues from the hunting habits of red foxes. When hunting, the red fox moves slowly towards its prey as it hides in the underbrush, and then it attacks the animal out of the blue. Like previous meta-heuristic models, this approach takes into account both the utilization and investigation of capabilities. This method creates random people for initializing parameters, as seen by the subsequent Eq. (3) and Eq. (4).

$$R = [r_0, r_1, \ldots . r_{n-1}] \tag{3}$$

$$(R)^i = [(r_0)^i, (r_1)^i \ldots . (r_{n-1})^i] \tag{4}$$

where, “I” denotes how many populations are present in the search area. Ten, the global optimal function is used to find the best solution in the search space. Here, the structure that follows is used in conjunction with the Euclidean distance to get the best solution as presented in Eq. (5).

$$E(((R)^i)^k, (R_{best})^k) = \sqrt{(R^i)^k - (R_{best})^k} \tag{5}$$

In Eq. (5) k denotes the number of iterations. The term "R_{best}t" represents the best optimum, while "E(.)" denotes the Euclidean distance. Accordingly, the optimal solution is employed to migrate all candidates, as illustrated in Eq. (6):

$$((R)^i)^k = ((R)^i)^k + g_{sign}((R_{best})^k - (R^i)^k)) \quad (6)$$

As a scaling hyperparameter, "g" denotes a random value selected at random from 0 to 1 for each iteration. For the whole population, this value is set just once every iteration. People evaluate the fitness values at their new places after moving to the optimal posture. People stay in their new roles if the fitness values are greater; if not, they return to their previous ones. This procedure is similar to how close relatives tell others where to hunt after an adventure and return home. They do what the explorers have instructed, going home "empty-handed" if they don't locate food, or continuing to search if there is a possibility. These processes, which take place during every DRF cycle, resemble suggested global inquiries. In addition, the applicants' move to new roles must present a feasible alternative; if not, their previous jobs will remain. The comparison of the red fox, advancing towards its prey and watches it, is appropriate here since it is similar to the DRF model in which a random number ω between 0 and 1 is assumed explained in Eq. (7) and Eq. (8) [24].

$$\begin{cases} Move\ Forward\ if, \omega > \frac{3}{4} \\ Stay\ Hiddem\ if, \omega > 3/4 \end{cases} \quad (7)$$

$$\omega = \begin{cases} \left\{ h \times \frac{\sin(\delta_0)}{\delta_0} \right. & if\ \delta_0 \neq 0 \\ \tau & if\ \delta_0 \neq 0 \end{cases} \quad (8)$$

Here, "h" is a random number in the interval [0, 0.2], and "δ0" is another random number in the interval [0, 2π], which indicates the fox viewing angle. Furthermore, "τ" represents a random number between 0 and 1. To model motions for the population of persons, the set of solutions for geographic coordinates is as follows. All things considered, the incorporation of RFO for picking features in intrusion detection systems improves computing efficiency and scalability while also strengthening the system's capacity to precisely detect and address security threats in Internet of Things networks. This method emphasises how crucial it is to use cutting-edge optimisation strategies in order to optimise feature subsets and improve intrusion detection technologies' overall effectiveness.

H. Intrusion Detection using Attention Bi-LSTM

The Attention-based BiLSTM model is used to identify intrusions in the NSL-KDD dataset. Using specialised memory units, LSTM—an improved version of the classic Recurrent Neural Networks (RNN)—captures long-term relationships in the MTS dataset efficiently [20]. The gradient vanishing problem is addressed by LSTM models, in contrast to conventional RNN techniques. Rather than depending just on the architecture of hidden units, they also incorporate memory cells that capture the long-term dependence of the signal. Four regulated gates make up the LSTM model: an output gate, a forget gate, input gate, in addition to a self-loop memory cell. These gates control how several memory neurons' data streams communicate with one another. The forget gate in the LSTM model's hidden layer decides which data from the previous time frame to keep and which to discard. The input gate makes the decision to simultaneously inject data from the memory unit into the input signal or not. The output gate decides whether to change the state of the memory unit [24]. The following Eq. (9) through Eq. (14) are used to determine the neuron state, hidden layer results, and gate states, taking into account the input xt from the NSL-KDD dataset and the dynamic output state h_t:

$$ip_t = \sigma(X_i u_t + Y_i h_{t-1} + a_i) \quad (9)$$

$$fg_t = \sigma(X_f u_t + Y_f h_{t-1} + a_f) \quad (10)$$

$$op_t = \sigma(X_o u_t + Y_o h_{t-1} + a_o) \quad (11)$$

$$c_t = fg_t \odot c_{t-1} + ip_t \odot \tilde{C}_t \quad (12)$$

The weight matrices that recur are indicated by as Y_i, Y_f, Y_o, while the representation of the weighted matrix for the forget, output, input, and memory cell gating by X_i, X_f, X_o, respectively. The biases for the gates are formulated as a_i, a_f, a_o. The candidate's cell state $\tilde{C}_t$, is utilized to update the original memory cell state, c_t. Step indicates the hidden layer's state h_{t-1}at any given moment, while ot indicates the outputop_t. The symbol ⊙ denotes the element-wise multiplication operation. The hyperbolic tangent function is denoted as tanh, and the logistic sigmoid activation function is represented by σ.

The standard LSTM model's limitation lies in its one-directional analysis of input signals during training, potentially leading to the inadvertent oversight of sequential information. In contrast, the BiLSTM was designed with a bidirectional structure, leveraging two LSTM layers operating in opposing directions to capture representation information both forwards and backwards. This bidirectional setup includes a hidden layer for reverse transmission (denoted as hb(t)), incorporating future values, alongside a forward propagation hidden layer (hf(t)) that retains data from previous sequence values. Ultimately, the BiLSTM model's final output is a fusion of both hf(t) and hb(t), facilitating a more comprehensive understanding of time series data.

$$M_{fg}(t) = \varphi\left(Y_{fm} u_t + Y_{fmm} u_{f(t-1)} + a_{fa}\right) \quad (13)$$

$$M_a(t) = \varphi\left(Y_{am} u_t + Y_{amm} u_{a(t-1)} + a_a\right) \quad (14)$$

Besides these, $a_{fa}$and $a_a$also relate to two-way biassed data. The weight matrix "Y_{fm} and Y_{am}"represents the synaptic weights from the input value to the internal unit for both forward and backward directions. Similarly, the forward and backward feedback recurrent weights are denoted by $Y_{fmm}$and Y_{amm}.

The tanh function serves as the activation function ψ for the hidden layers (HLs). It determines the output of the BiLSTM as b_t.

$$b_t = \sigma(W_{fmb} m_{f(t)} + W_{amb} m_{a(t)} + a_b) \quad (15)$$

The forward and backward weights of the resulting layers are represented by W_{fmb} and W_{amb}, respectively, in Eq. (15). Both a linear or sigmoidal function is provided as the

activation function of the resulting layer σ. Moreover, by denotes the bias in the output.The attention mechanism contributes to the learning process of the Attention BiLSTM model by assigning varying weights. The attention ai for a hidden layer hi is calculated using Eq. (16):

$$x_i = \tanh(Wh_i + a) \quad (16)$$

BiLSTM networks provide a powerful means to examine sequential data streams, enabling real-time detection of anomalous behavior and security threats in IoT networks. Leveraging BiLSTM architectures, these networks excel in capturing temporal dependencies and patterns present in IoT data, which are often characterized by their dynamic and time-varying nature. By effectively modelling the sequential nature of IoT data, BiLSTM networks can accurately identify deviations from normal behavior, facilitating prompt detection of intrusions and security breaches. To protect the integrity and confidentiality of IoT systems and devices, respond proactively to new threats, and strengthen the security posture of IoT networks, this capability is essential.

I. Blockchain Integration

The integration of blockchain technology into intrusion detection systems involves several key steps to ensure the integrity and immutability of the data while facilitating secure communication among distributed IoT devices through smart contracts.

1) Data logging: In the process of data logging, intrusion detection data generated by IoT devices is systematically recorded onto the blockchain network. Each piece of data is meticulously timestamped and cryptographically secured, ensuring its integrity and safeguarding against any potential tampering attempts. By timestamping each entry, the blockchain network establishes a chronological order of events, enabling a comprehensive audit trail of intrusion activities. Additionally, the cryptographic security measures implemented within the blockchain network guarantee the immutability of the logged data, thereby providing a reliable and tamper-proof record of security events. This meticulous logging process enhances the trustworthiness and reliability of the intrusion detection system, enabling robust security monitoring in IoT networks [25].

2) Blockchain node: In the context of blockchain technology, blockchain nodes serve as essential components responsible for validating and recording logged intrusion detection data. These nodes are distributed across the blockchain network, ensuring decentralization and resilience against single points of failure. Each node maintains a copy of the decentralized ledger, which contains a complete record of all transactions, including the logged intrusion detection data. When new data is logged onto the blockchain, it undergoes validation by multiple nodes within the network to ensure its authenticity and integrity. This validation process involves verifying the cryptographic signatures associated with the data and confirming its adherence to the consensus rules established by the network protocol. Once validated, the intrusion detection data is appended to the blockchain ledger, becoming a permanent and immutable part of the distributed database. By distributing the responsibility for data validation and storage among multiple nodes, blockchain networks achieve redundancy and fault tolerance, enhancing the reliability and resilience of the overall system. Furthermore, as blockchain nodes are decentralised, no one organisation can exert control over the system as a whole, fostering openness, confidence, and security in the logging and archiving of intrusion detection data.

3) Proof of work: The consensus mechanism of the blockchain is essential to guaranteeing that all dispersed nodes agree on the veracity of logged data. To reach this consensus among network users, consensus techniques like Proof of Work (PoW) are used. Proof-of-work (PoW) consensus is a competitive mechanism in which nodes solve challenging mathematical problems to validate transactions and append new blocks to the blockchain. This is a resource-intensive procedure that uses a lot of energy and processing power. Nonetheless, other nodes in the network confirm the answer after a node completes the puzzle and suggests a new block. The block is appended to the blockchain if the answer satisfies the consensus requirements. By using this decentralised method, blockchain networks maintain the integrity and durability of the blockchain ledger by facilitating consensus across dispersed nodes about the veracity of recorded data. Additionally, consensus mechanisms like PoW contribute to the security of the blockchain network by mitigating the risk of malicious actors attempting to manipulate or alter the logged data. Overall, the consensus mechanism serves as a fundamental building block of blockchain technology, enabling decentralized trust and coordination among network participants [26].

A key element of blockchain networks is the proof-of-work (PoW) consensus mechanism, which guarantees dispersed nodes' agreement on the legitimacy of transactions and the appending of new blocks to the blockchain. PoW comprises the following crucial steps:

- Transaction Propagation: Transactions are broadcasted to all nodes in the blockchain network. Each transaction contains details such as sender, recipient, amount, and cryptographic signatures.
- Block Creation: Transactions are grouped together into blocks, forming a candidate block for addition to the blockchain. Miners, who are nodes responsible for creating new blocks, select transactions and assemble them into a block structure.
- Mining Competition: Miners compete with each other to solve the Proof of Work puzzle. They utilize computational power to generate hash values by iteratively modifying a nonce (a random number) in the block header until the desired hash value is found. This process is computationally intensive and requires significant computational resources.

- Verification: A miner broadcasts the candidate block and the solution to the network as soon as they discover a workable solution to the problem. The legitimacy of the answer and the transactions included in the block are then confirmed by further nodes inside the network.
- Consensus: If the majority of nodes in the network agree that the proposed solution is sound and the block conforms to the consensus requirements, the block is accepted and posted to the blockchain. It is ensured that all distributed nodes concur on the validity of the transactions and the addition of new blocks to the blockchain by going through this process.
- Reward: A fixed quantity of bitcoin plus any transaction fees included in the block are awarded to the miner who effectively mines a new block. This encourages miners to use up processing power and take part in the consensus-building process on the network.

In general, the Proof of Work technique reduces the possibility of malevolent actors attempting to influence the blockchain by demanding computational resources to verify transactions and generate new blocks, hence ensuring the security and integrity of blockchain networks.

1) Smart contract: Smart contracts serve as the backbone of automation and governance within IoT networks by providing a decentralized, programmable framework for enforcing rules and conditions. These contracts, encoded with predefined logic, are deployed on the blockchain, ensuring immutability and tamper-proof execution. Within the context of IoT, smart contracts automate interactions between devices, enabling seamless communication and coordination without the need for intermediaries. By executing automatically when specific conditions are met, such as sensor readings or trigger events, smart contracts streamline processes and mitigate the risk of human error. Moreover, the decentralised structure of these systems gets rid of single points of failure and minimises dependence on centralised authority, hence improving security and resilience. Additionally, conditional execution of operations is made possible by smart contracts, which let gadgets react quickly to shifting conditions. This feature improves IoT network responsiveness and operational efficiency. Furthermore, network participants' confidence and responsibility are bolstered by the openness and auditability provided by smart contracts. Overall, smart contracts play a critical role in driving efficiency, security, and transparency in IoT ecosystems, laying the foundation for scalable and resilient decentralized applications [27].

2) Secure communication: In the ecosystem of IoT networks, secure communication is facilitated through the interaction between IoT devices and the blockchain network via smart contracts. These contracts act as intermediaries, enforcing cryptographic protocols and access controls to ensure that communication remains secure. By leveraging cryptographic techniques such as encryption and digital signatures, smart contracts authenticate and authorize devices, mitigating the risk of unauthorized access or tampering. Through predefined rules and conditions encoded within the smart contracts, only authorized devices are granted permission to access and modify data stored on the blockchain. This robust enforcement of security measures enhances the integrity and confidentiality of communication within IoT networks, safeguarding sensitive information and preventing unauthorized manipulation of data. Overall, the utilization of smart contracts enables secure and trustworthy communication channels, fostering confidence in the exchange of data and transactions within IoT ecosystems.

V. Result and Discussion

The proposed framework undergoes rigorous evaluation using benchmark datasets, including NSL-KDD and BoT-IoT, to comprehensively assess its performance in detecting various types of intrusions within IoT networks. By leveraging these datasets, which contain diverse and realistic intrusion scenarios, the framework's efficacy in identifying and mitigating security threats is thoroughly scrutinized. Performance metrics are used to assess how well the framework differentiates between malicious activity and typical network behavior. These measures include detection accuracy, false positive rate, and computing efficiency. Furthermore, the assessment procedure entails contrasting the outcomes of the framework with those of current intrusion detection systems in order to measure its effectiveness in relation to predetermined benchmarks. The suggested framework's potential to strengthen the security posture of IoT networks is carefully investigated through this methodical study utilizing typical datasets, offering insights into its advantages and shortcomings.

A. Performance Metrics

Performance metrics refer to the numerical values that are utilized to assess how well an intrusion detection system detects and neutralizes security threats on a network. Commonly used metrics include the following ones:

1) Accuracy: The percentage of accurately identified occurrences—both true positives and true negatives—out of all the instances that were examined is known as accuracy. It offers a general indicator of how effectively the intrusion detection system classifies events as either intrusions or routine activity.

2) Precision: Positive predictive value, or precision, is a metric that expresses the percentage of accurately detected positive cases (true positives) across every case categorized as positive (false positives and true positives). It shows how well the system can detect intrusions without mistakenly labelling routine operations as such.

3) Recall: Recall, also known as sensitivity or true positive rate, is the proportion of correctly identified positive cases relative to all real positive occurrences in the dataset. It assesses the system's ability to identify every incursion, lowering the likelihood that any malicious activity would go undetected.

4) F1-score: The F1-score, which achieves equilibrium between recall and accuracy, is derived from the harmonic mean of these two metrics. Recall and accuracy are combined into one figure, which accounts for both false positives and false negatives.

TABLE I. PERFORMANCE METRICS

Metrics	Efficiency
Accuracy	98.9
Precision	94
Recall	95
F1-Score	95

As shown in Table I and Fig. 2, the suggested intrusion detection approach exhibits excellent efficiency with an accuracy of 98.9%, demonstrating its capacity to accurately categorise cases as either intrusions or routine operations. Furthermore, the approach displays a 94% accuracy rate, which indicates the percentage of accurately detected incursions among all cases that are categorised as positive, hence reducing false positives. With a recall rate of 95%, which indicates that the system can detect all incursions, there is little chance of a missed detection. Furthermore, a balanced performance in terms of both accuracy and recall is shown by the F1-score, which harmonises the two metrics, which is recorded at 95%. All of these measures show how successful and dependable the suggested intrusion detection technique is at identifying and reducing security risks in the network infrastructure.

Fig. 2. Performance efficiency.

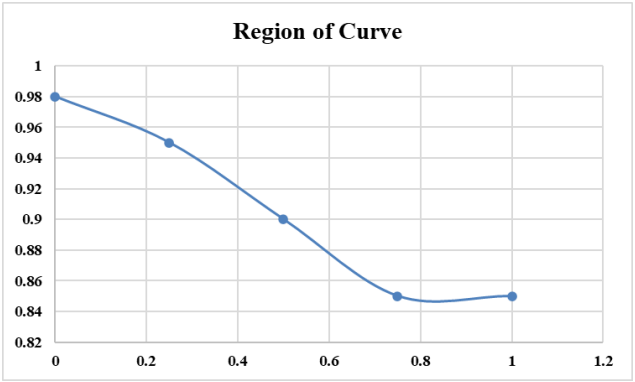

Fig. 3. Receiver operating characteristic curve.

As the threshold rises from 0 to 1, the true positive rate (TPR) progressively falls from 0.98 to 0.85, suggesting a decline in the percentage of true positive cases that are correctly categorised, as seen in Fig. 3. The TPR stays comparatively high at 0.95 at a threshold of 0.25, indicating that true positive cases can be effectively detected even with somewhat loosened thresholds.

TABLE II. SORTING RESULT OF NSL-KDD

Methods	AUC	Error Rate
Gradient Boosting Classifier	47.64	0.4905
Deep Learning	77.88	0.2256
Proposed Method	98.9	0.0025

The NSL-KDD dataset's categorization outcomes using different techniques are shown in Table II. With an error rate of 0.4905 and an AUC of 47.64%, the Gradient Boosting Classifier performs relatively poorly. By comparison, the Deep Learning approach shows noticeably higher performance, with an error rate of 0.2256 and an AUC of 77.88%.

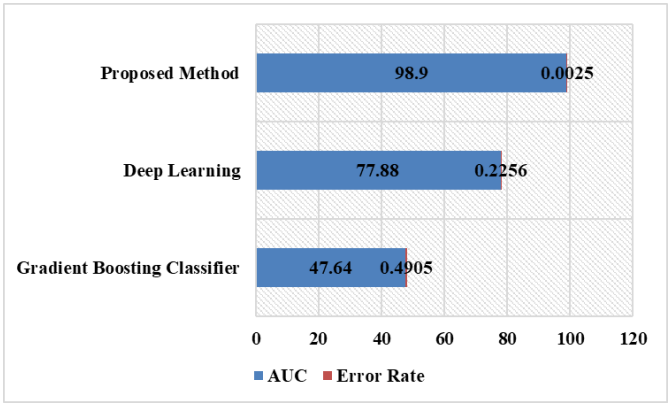

Fig. 4. Classification result of NSL-KDD.

The results presented in Fig. 4 demonstrate that the suggested approach outperforms the two other options, with an exceptional AUC of 98.9% and a remarkably low error rate of 0.0025. These outcomes highlight how well the suggested strategy performs in comparison to other methods when it comes to correctly identifying instances in the NSL-KDD dataset.

TABLE III. RECOGNITION OUTCOMES OF ATTENTION BASED BILSTM APPROACH ON NSL-KDD DATASET

Data	Class	Accuracy	Precision	Recall	F1-Score
Training	*Normal*	98.4	96.3	97.3	96.3
	Attack	97.4	97.4	98.4	95.5
	Average	97.7	97.7	97.7	97.7
Testing	*Normal*	98.9	97.5	96.4	95.8
	Attack	97.3	98.3	97.3	98.3
	Average	98.9	98.9	98.9	98.9

The NSL-KDD dataset's recognition results from the Attention-based BiLSTM technique are shown in Table III and Fig. 5.

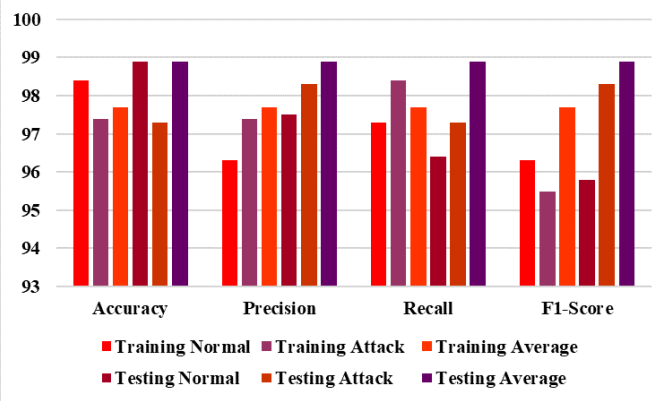

Fig. 5. Recognition outcomes of attention based BiLSTM approach on NSL-KDD dataset.

It includes accuracy, precision, recall, and F1-Score, split into normal and attack classes, for both the training and testing datasets. In the training dataset, the method achieves 98.4% accuracy for normal cases and 97.4% accuracy for attack instances. Respectively, the corresponding accuracy, recall, and F1-Score values are 95.5% and 96.3%, 97.3% and 98.4%, and 96.3% and 97.4%. Comparable outcomes are seen in the testing dataset, where the technique achieves 97.3% accuracy for attack instances and 98.9% accuracy for normal cases. The corresponding F1-Score, recall, and accuracy scores are 97.5%, 98.3%, and 95.8%, respectively. The average results for each class are also provided for the training and testing datasets.

B. Discussion

The research studies under discussion offer novel strategies for resolving the security issues that arise in Internet of Things networks. These specifically concentrate on intrusion detection systems (IDS) and make utilisation of blockchain and machine learning technology. The study by Liang et al. [12] suggests a hybrid intrusion detection system that makes use of multi-agent systems, blockchain technology, and deep learning techniques. The system is divided into distinct modules for data collecting, management, analysis, and response with the goal of improving detection accuracy, particularly at the transport layer of Internet of Things networks. Scalability and optimisation continue to be major obstacles to practical implementation, notwithstanding encouraging findings. A collaborative intrusion detection architecture including blockchain technology for safe sharing of threat intelligence across cloud and Internet of Things networks is presented by Alkadi et al. [13]. While consensus processes and deep blockchain technology are adept at detecting intrusions and reducing security threats, their scale presents serious problems for efficiency and real-time response. A blockchain-based collaborative signature-based IDS called CBSigIDS is proposed by Li et al. with the goal of creating a trustworthy signature database in dispersed IoT systems. Although it provides a safe way to validate signatures, blockchain overhead scalability issues require further work before a viable implementation can be made. Kumar et al. [14] offers a distributed intrusion detection system (IDS) that uses blockchain technology and fog computing to identify DDoS assaults directed at IoT mining pools. They assess the system's effectiveness in identifying IoT network assaults using machine learning algorithms trained on scattered fog nodes. But there are still issues with realistic implementation and optimisation needed for efficiency and scalability. Although these studies show how blockchain and machine learning technologies could potentially use to improve IoT network security, scalability, optimisation, and practical deployment issues must be resolved before their full promise could be realised in practical settings.

The study presents a complete framework for reliable and scalable intrusion detection in IoT networks by integrating machine learning techniques with blockchain technology. The solution addresses the challenges posed by the dynamic and heterogeneous nature of IoT environments by employing Red Fox Optimization for feature selection and Attention-based BiLSTM for anomaly identification. The adoption of blockchain technology improves security by ensuring the validity and inviolability of intrusion record detection. The study advances the area by providing an all-encompassing method of intrusion detection that takes security and efficiency into account. Real-time identification of abnormalities and malicious activity in IoT traffic is made possible by the use of sophisticated machine learning algorithms, and scalability is improved by optimization approaches that assist decrease the dimensionality of the input data. Furthermore, the system gains an additional degree of protection through the integration of the technology known as blockchain, which offers tamper-resistant recordings of detected intrusions. The usefulness of the suggested architecture is demonstrated by experimental findings, which on real-world IoT datasets yield a high detection accuracy of about 98.9%. These findings highlight how important the study is to improving IoT security state-of-the-art. The report does, however, admit several limitations, including the need for more assessment in various IoT scenarios and the computational cost related to blockchain integration. Prospective study avenues encompass investigating alternative machine learning algorithms and optimization methods, tackling scalability issues, and refining blockchain-associated procedures. Overall, the research offers a viable strategy for improving intrusion detection in Internet of Things networks, opening the door to more robust and safe linked settings.

VI. CONCLUSION

The suggested system, which makes use of blockchain and machine learning, offers a viable solution to the problems associated with intrusion detection in Internet of Things networks. The accuracy and scalability of the intrusion detection system are improved by integrating Red Fox Optimization for feature selection and Attention-based BiLSTM for anomaly detection. Moreover, the incorporation of blockchain technology ensures the integrity and immutability of intrusion detection logs, thereby enhancing security. On real-world IoT data sets, experimental findings show the usefulness of the technique with a high detection

accuracy of about 98.9%. However, it is important to acknowledge some limitations and areas for future work. Firstly, while the proposed framework shows promising results, further research is needed to evaluate its performance in diverse IoT environments and under various attack scenarios. Additionally, the scalability of the system needs to be investigated to handle large-scale IoT networks efficiently. Furthermore, the computational overhead associated with blockchain integration may pose challenges in resource-constrained IoT devices, requiring optimization strategies. Moreover, continuous advancements in intrusion techniques necessitate ongoing updates and improvements to the detection algorithms and feature selection methods. Future studies may look at applying more machine learning algorithms and optimization techniques to enhance the robustness and efficiency of intrusion detection systems in Internet of Things networks. All things considered, this work establishes the groundwork for next investigations that seek to create IoT ecosystems that are more robust and safer.

REFERENCES

[1] P. Raj and A. C. Raman, The Internet of Things: Enabling technologies, platforms, and use cases. Auerbach Publications, 2017.

[2] V. E. Balas and S. Pal, Healthcare Paradigms in the Internet of Things Ecosystem. Academic Press, 2020.

[3] Y. Liao, C. Thompson, S. Peterson, J. Mandrola, and M. S. Beg, "The future of wearable technologies and remote monitoring in health care," Am. Soc. Clin. Oncol. Educ. Book, vol. 39, pp. 115–121, 2019.

[4] A. Karale, "The challenges of IoT addressing security, ethics, privacy, and laws," Internet Things, vol. 15, p. 100420, 2021.

[5] A. Qasem, P. Shirani, M. Debbabi, L. Wang, B. Lebel, and B. L. Agba, "Automatic vulnerability detection in embedded devices and firmware: Survey and layered taxonomies," ACM Comput. Surv. CSUR, vol. 54, no. 2, pp. 1–42, 2021.

[6] R. Krishnamurthi, A. Kumar, D. Gopinathan, A. Nayyar, and B. Qureshi, "An overview of IoT sensor data processing, fusion, and analysis techniques," Sensors, vol. 20, no. 21, p. 6076, 2020.

[7] A. Riah, S. Daniel, E. Frank, and K. Seriffdeen, "The role of technology in shaping user behavior and preventing phishing attacks," 2024.

[8] T. M. Alshammari and F. M. Alserhani, "Scalable and Robust Intrusion Detection System to Secure the IoT Environments using Software Defined Networks (SDN) Enabled Architecture," Int J Comput Netw. Appl, vol. 9, no. 6, pp. 678–688, 2022.

[9] M. Javed, N. Tariq, M. Ashraf, F. A. Khan, M. Asim, and M. Imran, "Securing Smart Healthcare Cyber-Physical Systems against Blackhole and Greyhole Attacks Using a Blockchain-Enabled Gini Index Framework," Sensors, vol. 23, no. 23, p. 9372, 2023.

[10] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers," in Proceedings of the Seventh International Conference on the Internet of Things, 2017, pp. 1–8.

[11] A. K. Al Hwaitat et al., "A New Blockchain-Based Authentication Framework for Secure IoT Networks," Electronics, vol. 12, no. 17, p. 3618, Aug. 2023, doi: 10.3390/electronics12173618.

[12] C. Liang et al., "Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems," Electronics, vol. 9, no. 7, p. 1120, Jul. 2020, doi: 10.3390/electronics9071120.

[13] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," IEEE Internet Things J., vol. 8, no. 12, pp. 9463–9472, 2020.

[14] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network," J. Parallel Distrib. Comput., vol. 164, pp. 55–68, Jun. 2022, doi: 10.1016/j.jpdc.2022.01.030.

[15] H. Vargas, C. Lozano-Garzon, G. A. Montoya, and Y. Donoso, "Detection of Security Attacks in Industrial IoT Networks: A Blockchain and Machine Learning Approach," Electronics, vol. 10, no. 21, p. 2662, Oct. 2021, doi: 10.3390/electronics10212662.

[16] R. H. Hylock and X. Zeng, "A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study," J. Med. Internet Res., vol. 21, no. 8, p. e13592, Aug. 2019, doi: 10.2196/13592.

[17] "NSL-KDD." Accessed: Mar. 21, 2024. [Online]. Available: https://www.kaggle.com/datasets/hassan06/nslkdd.

[18] H. Moudoud, S. Cherkaoui, and L. Khoukhi, "An IoT blockchain architecture using oracles and smart contracts: the use-case of a food supply chain," in 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, 2019, pp. 1–6.

[19] P. Bari and P. Karande, "Application of PROMETHEE-GAIA method to priority sequencing rules in a dynamic job shop for single machine," Mater. Today Proc., vol. 46, pp. 7258–7264, 2021, doi: 10.1016/j.matpr.2020.12.854.

[20] P. Yazdanian and S. Sharifian, "E2LG: a multiscale ensemble of LSTM/GAN deep learning architecture for multistep-ahead cloud workload prediction," J. Supercomput., vol. 77, pp. 11052–11082, 2021.

[21] F. Karim, S. Majumdar, and H. Darabi, "Insights Into LSTM Fully Convolutional Networks for Time Series Classification," IEEE Access, vol. 7, pp. 67718–67725, 2019, doi: 10.1109/ACCESS.2019.2916828.

[22] Z. Ahamed, M. Khemakhem, F. Eassa, F. Alsolami, and A. S. A.-M. Al-Ghamdi, "Technical Study of Deep Learning in Cloud Computing for Accurate Workload Prediction," Electronics, vol. 12, no. 3, p. 650, 2023.

[23] E. S. P. Krishna and A. Thangavelu, "Attack detection in IoT devices using hybrid metaheuristic lion optimization algorithm and firefly optimization algorithm," Int. J. Syst. Assur. Eng. Manag., May 2021, doi: 10.1007/s13198-021-01150-7.

[24] R. AlGhamdi, "Design of Network Intrusion Detection System Using Lion Optimization-Based Feature Selection with Deep Learning Model," Mathematics, vol. 11, no. 22, p. 4607, Nov. 2023, doi: 10.3390/math11224607.

[25] S. Rathore, J. H. Park, and H. Chang, "Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT," IEEE Access, vol. 9, pp. 90075–90083, 2021, doi: 10.1109/ACCESS.2021.3077069.

[26] A. H. Sodhro, S. Pirbhulal, M. Muzammal, and L. Zongwei, "Towards blockchain-enabled security technique for industrial internet of things based decentralized applications," J. Grid Comput., vol. 18, pp. 615–628, 2020.

[27] B. Yin, Y. Wu, T. Hu, J. Dong, and Z. Jiang, "An efficient collaboration and incentive mechanism for Internet of Vehicles (IoV) with secured information exchange based on blockchains," IEEE Internet Things J., vol. 7, no. 3, pp. 1582–1593, 2019.