Unleashing the power of Bat optimized CNN-BiLSTM model for advanced network anomaly detection: Enhancing security and performance in IoT environments

by Antonius Alijoyo

Submission date: 03-Nov-2025 08:29AM (UTC+0700)
Submission ID: 2801107522
File name: ing_the_power_of_Bat_optimized_CNN-BiLSTM_model_for_advanced.pdf (1.8M)
Word count: 7707
Character count: 41708

Alexandria Engineering Journal 84 (2023) 333–342

Contents lists available at ScienceDirect

Alexandria Engineering Journal

journal homepage: www.elsevier.com/locate/aej

Original Article

Unleashing the power of Bat optimized CNN-BiLSTM model for advanced network anomaly detection: Enhancing security and performance in IoT environments

Franciskus Antonius [a,*], J.C. Sekhar [b], Vuda Sreenivasa Rao [c], Rahul Pradhan [d], S. Narendran [e], Ricardo Fernando Cosio Borda [f], Susan Silvera-Arcos [f]

[a] School of Business and Information Technology STMIK LIKMI, Bandung Indonesia
[b] NRI Institute of Technology, Guntur, India
[c] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation Vaddeswaram, AP, India
[d] Department of Computer Engineering and Applications, GLA University, Mathura, India
[e] Dept of Nanotechnology, Institute of Electronics and Communication Engineering, SIMATS Engineering, Saveetha Institute of Medical and Technical Sciences, Kanchipuram, India
[f] Universidad Privada del Norte, Peru

ARTICLE INFO

Keywords:
Internet of Things (IoT)
Bidirectional Long Short-Term Memory (BiLSTM)
Convolutional Neural Network (CNN)
Particle Swarm Optimisation (PSO)
Anomaly Detection

ABSTRACT

The growth of IoT (Internet of Things) devices has revolutionized several industries and brought about novel security threats. Recognizing network anomalies that may point to malicious activity or system flaws is a major issue. Traditional anomalous identification methods frequently need to catch up when dealing with the special traits of IoT environments, including resource limitations and changing network behavior. This paper introduces an innovative approach, the Bat-optimized CNN-BiLSTM model, to enhance the security and efficiency of IoT environments. This model combines the strengths of Convolutional Neural Networks (CNNs) for spatial analysis and Bidirectional Long Short-Term Memory (BiLSTM) networks for capturing temporal patterns, thus effectively representing time and space trends in IoT data. To optimize its performance further, researchers have leveraged the Bat algorithm, inspired by natural behaviors, to fine-tune the model. This program effectively searches for the best network anomaly detection parameters by imitating the echo activity of bats. Researchers want to increase detection accuracy by lowering false positives and false negatives using the Bat algorithm to enhance the CNN-BiLSTM model. The experimental findings show that the Bat-optimised CNN-BiLSTM model beats the state-of-the-art anomaly detection methods with 99.43% accuracy and efficiency.

1. Introduction

The IoT has evolved as a game-changing technology that enables countless gadgets and systems in various fields, including intelligent homes, automation in industry, healthcare, and travel, to be connected. IoT device usage has increased effectiveness and ease like never before but has also brought about new security risks. Identifying network anomalies represents one of the most important issues in IoT systems. Anomalies in network performance can indicate malicious activity, including intrusion attempts, Distributed Denial of Service (DDoS) assaults, and system errors or errors in configuration. The safety and reliability of IoT systems depend on promptly identifying these anomalies. In the last few years, the growth of the Internet of Things, or IoT, gadgets have revolutionized multiple sectors by bringing unparalleled connection and ease. Yet, as IoT adoption has increased exponentially, network security flaws have additionally come to light, necessitating the development of strong anomaly detection solutions to protect these linked environments [1]. The numerous device kinds, enormous data volumes, and dynamic network topologies offered by the Internet of Things (IoT) provide special issues that conventional approaches to identifying anomalies find difficult to address. Therefore, it is imperative to investigate cutting-edge technologies that improve efficiency and safety in IoT contexts.

Conventional computer networks have extensively used mathematical methodologies and rule-based systems for anomaly identification. Due to their inability to properly deal with the distinctive properties of

* Corresponding author.
E-mail address: franciskus.antonius.alijoyo63@gmail.com (F. Antonius).

https://doi.org/10.1016/j.aej.2023.11.015
Received 21 July 2023; Received in revised form 18 October 2023; Accepted 3 November 2023
Available online 27 November 2023
1110-0168/© 2023 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Engineering, Alexandria University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

IoT networks, these strategies are frequently inadequate for IoT contexts. IoT networks include dynamic behaviors, a variety of data forms, and resource limitations, all of which call for the creation of specialized anomaly detection methods. Convolutional and recurrent networks of neurons, in particular, have achieved outstanding results in several fields, such as speech recognition, natural language processing, and computer vision. Though RNNs, particularly the BiLSTM networks, are skilled at catching temporal connections in sequential information, CNNs excel in extracting spatial trends from structured information [2].

In this paper, researchers suggest a fresh method for overcoming network detection of anomalies difficulties in IoT situations. By combining the advantages of CNNs with BiLSTM networks, researchers unlock the power of a Bat-optimised CNN-BiLSTM model to detect geographical and temporal trends in network traffic data. Researchers use the Bat algorithm, a nature-inspired optimisation method, to further improve the suggested technique's efficiency. The Bat algorithm imitates how bats use echoes to locate prey effectively by emitting ultrasonic waves and varying the frequency and intensity. Similarly, the Bat algorithm optimizes the CNN-BiLSTM model's parameters to increase detection accuracy by reducing false positives and negatives. The deployment of a Bat-Optimized CNN along with a BiLSTM approach to network anomaly detection in the Internet of Things (IoT) ecosystem is suggested in this paper as a solution to these problems [3]. Because of its effectiveness and adaptability, the Bat algorithm, modeled after the foraging behavior of bats, has become well-known in optimization challenges. The suggested approach, which takes advantage of the Bat algorithm's optimization capacity, is created to maximize the detection's precision while reducing the computation's complexity, making it appropriate for continuous tracking in the Internet of Things (IoT) setting. The anomaly detection in IoT data is shown in the Fig. 1.

This research aims to improve security and performance in IoT contexts through improved network anomaly detection. We seek to overcome the shortcomings of conventional anomaly detection methods and create an effective approach capable of identifying and managing network anomalies in IoT systems by utilizing the Bat-optimised CNN-BiLSTM model. Using a real-world IoT dataset with a wide variety of network anomalies, we assess the performance of our suggested model. They compared the findings to show that our method is better than other anomaly detection methods. We also consider the resource limitations of IoT devices and optimize the model to reduce computational overhead, making it appropriate for implementation in IoT contexts with limited resources [4]. For enhanced network detection of anomalies in IoT scenarios, this research introduces a unique Bat-Optimized CNN-BiLSTM model. Researchers seek to improve safety and efficiency in IoT ecosystems by utilizing the advantages of the Bat algorithm and the integrated CNN-BiLSTM design. This will eventually decrease the dangers related to network abnormalities and guarantee the continuous functioning of vital devices.

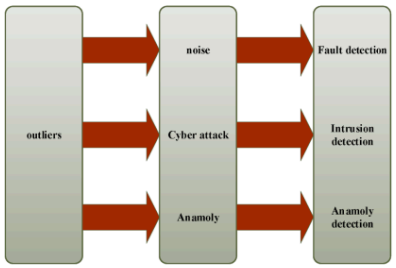


Fig. 1. Anamoly detection in IOT data.

There are undoubtedly several compelling benefits to using deep learning for detecting anomalies in IoT. CNNs in long LSTM networks are examples of deep learning models that excel at capturing complicated, non-linear trends in data, which is essential for spotting subtle and developing anomalies in IoT contexts. Deep learning models can respond to changing network behaviors, which makes them stronger in the dynamic IoT landscape than conventional rule-based or statistical approaches. Deep learning can process various data kinds, including text, pictures, and sensor readings, frequently used in IoT installations. This adaptability makes it possible to detect anomalies holistically across different kinds of IoT devices and data sources, giving a full picture of the network's condition. Furthermore, the extraction of features and representation learning tasks can be carried out by deep learning models, which eliminates the requirement for manually created feature engineering and increases the approach's scalability and flexibility. The BiLSTM networks' bidirectional nature improves the model's capacity to identify temporal dependence, which is essential for spotting abnormalities that change over time. Overall, deep learning is a powerful solution for solving the particular difficulties of IoT detection of anomalies. It gives greater precision and flexibility than conventional approaches since it is data-driven and flexible.

The incorporation of CNN and BiLSTM architectures forms the basis of the suggested model. CNNs are especially well-suited for collecting geographic trends in internet traffic information because they are excellent at identifying high-level characteristics from unstructured data. The ability to capture time-dependent and contextual data is a strength of BiLSTM networks, which enables a richer comprehension of sequence input. By merging the two designs, this model may use spatial and temporal properties, making anomaly identification more precise and thorough. Enhancing anomaly detection precision, lowering false positive rates, and increasing computing efficiency are the three main goals of the suggested approach. Meeting these goals is essential for guaranteeing the stability and dependability of IoT networks because false positives may result in pointless alarms triggering, and erroneous negatives can cause safety breaches that aren't discovered [5]. By concurrently collecting spatial and temporal patterns—CNNs handle spatial characteristics, and BiLSTM networks model temporal relationships—CNN-BiLSTM excels at IoT anomaly identification. The model can reflect complicated geographical-temporal trends because of this all-encompassing approach, which is essential for locating anomalies with both spatial and temporal properties. Comparing CNN-BiLSTM to models that only focus on spatial or temporal elements, BiLSTM's capacity to detect anomalies across time is strengthened by its bidirectional nature.

The key contributions of this study are summarised as,

1. The Bat-optimized CNN-BiLSTM, a cutting-edge anomaly detection model specifically designed for IoT contexts, is presented in the study. It skillfully integrates CNNs for spatial evaluation and BiLSTM network for temporal structure modeling, enabling the collection of temporal and spatial trends in IoT data.
2. Modify the parameters of the suggested model by including the Bat algorithm, which was inspired by the behavior of natural echoes.
3. By efficiently looking for the best network parameters, this optimization technique seeks to improve the model's efficacy in anomaly detection while lowering false positives and negatives.
4. The study shows the efficiency of the Bat-optimized CNN-BiLSTM model through extensive testing on actual IoT datasets. It outperforms state-of-the-art techniques in detecting anomalies with a remarkable accuracy rate.
5. The high accuracy demonstrates the efficacy and practical usability of the suggested method for boosting security in IoT contexts.

The rest of the paper is summarised as follows: A description of relevant work in network anomaly detection and deep learning-based methods is given in Section 2. The problem statement is described in

section 3. The design of the Bat-optimised CNN-BiLSTM model and the implementation of the Bat algorithm are both covered in detail in the methodology. The experimental setup, dataset description, and evaluation assessment are explained in Section 4. The final results are discussed and contrasted with current methods in Section 5. The work is concluded in Section 6, which also suggests future study directions.

2. Related works

IoT (Internet of Things) technologies are already standard in many business and government sectors. Unfortunately, safety threats focusing on information integrity and service availability often target IoT devices and networks because of their high vulnerability. In addition, compared to traditional Information Technology (IT) networks, the diversity of information gathered from diverse IoT devices and the disruptions experienced inside the IoT system make it more difficult to spot aberrant behavior and hacked nodes. There is an urgent need for robust and trustworthy anomaly detection to ensure that fraudulent data won't be used in IoT-driven decision support systems. Abusitta et al. [6] propose IoT anomaly detection using deep learning because it may acquire and collect reliable and practical features without being greatly impacted by unpredictable situations. The classifier then uses these traits to improve the precision with which it can identify fraudulent IoT data. In particular, a denoising automatic encoder is used in the suggested deep learning algorithm's design to provide characteristics resistant to the IoT environment's heterogeneity. The suggested framework's efficacy in improving the precision of identifying malicious data compared to the most advanced IoT-based anomaly recognition models is demonstrated by experimental findings based on reality IoT datasets. This method is not robust, and it has a security problem.

The IoT is being used in several crucial areas to enhance the quality of services and simplify people's lives. The Internet of Things movement has transformed digital services across various industries through improved output, efficacy, and affordability. IoT security concerns remain a serious difficulty even though numerous companies have adopted IoT systems or aim to incorporate them as essential components of their systems' performance. Anomaly detection using machine learning may serve as an efficient security measure to combat a variety of IoT cyberattacks and reduce the risk of assaults on IoT networks. Although numerous detection approaches have been developed and put out in research, the ones now in use only target a small number of cyberattacks and base their assessments on out-of-date datasets. Alanazi et al.[7] Proposed a smart, efficient, portable detection method to catch various IoT assaults. To create a successful and effective detection model, our suggested model contains an open features selection process that chooses the best distinguishing characteristics and removes unneeded characteristics. Researchers also suggested a combination of learning algorithms to enhance classifications for foretelling various sorts of IoT assaults during the identification phase. The study outcomes demonstrate that the proposed strategy can accurately and effectively anticipate several IoT assaults with higher rates of 99.983 % F1-score, 99.984 % accuracy, 99.984 % recall, and 99.982 % precision. This method is effective even though it improves the effectiveness and accuracy by performing experimental evaluations.

The large development of IoT and AI technology results in an overabundance of communication information that is not handled promptly, which poses a possible danger to intelligent cities. Since it is a crucial component of cyber safety for operations provided by smart cities, the study regarding how to best use this information for anomaly detection is gaining popularity. The current methods frequently ignore the impact of poor detection precision brought on by drift phenomena and instead concentrate on static information for identifying anomalies or data that streams. Xu et al.[8] Focus on the issue of anomaly detection in smart city services and effectively differentiate between them to safeguard the security of user information. Then, suggest a ground-breaking notion for drift adaptable methodology that completely considers how time affects the distribution of samples along a timeline to increase the precision of anomaly detection. Additionally, offer an AI-based Improved Long-Term Memory (I-LSTM) neural network with a new smoothing activation mechanism and additional time to enhance the accuracy of multiple class for anomaly detection. Finally, a real communication dataset is used to assess our suggested solutions. According to comprehensive research results, I-LSTM has the highest metrics scores. This indicates the efficacy of the suggested techniques that may deliver a smart city with outstanding quality of service, resulting in an ideal combination of security of communication and artificial intelligence. Enhancing the multiclassification method is necessary to increase the robustness of this strategy.

In commercial cyber-physical systems (CPS), AI and smart approaches are being utilized and have grown in popularity with Industry 4.0's growing population. Smart anomaly detection remains a difficult problem, particularly when working with limited labeled information for cyber-physical security purposes. This is necessary to spot cyber-physical threats and ensure work effectiveness and security. Zhou et al.[9] Proposed to address the problem of over-fit and improve efficiency for intelligent anomaly detection in commercial CPS, a few-shot learning model with Siamese convolutional neural network (FSL-SCNN) was developed. A Siamese CNN encoding network is built to calculate incoming sample lengths depending on their optimized feature depictions. The effectiveness of the instruction method is then improved with the proposal of a strong cost-functional architecture that includes three different losses. Lastly, a sophisticated anomaly detection algorithm is created. The results of our experiments show that the suggested FSL-SCNN may greatly reduce the rate of false alarms (FAR) and F1 scores while identifying intrusion signs for commercial CPS security purposes. The experiments were conducted on an entirely labeled open dataset and some labeled datasets. More algorithm assessments are conducted under various conditions to increase accuracy and efficiency.

The rapid growth of IoT (Internet of Things) generates many communications information. Such enormous amounts of data aren't processed promptly, making smart services anomaly detection more challenging. Labeling every piece of transmission data is also impractical. Thus, it is important to implement certain workable methods that may efficiently include unlabelled data. The Temporal Convolutional Network (TCN), recently introduced to address sequence issues, performs better than Recurrent Neural Networks (RNN) in most scenarios. Cheng et al.[10] Proposed, for the very first time, a semi-supervised hierarchy stacked TCN that focuses on communications anomaly detection in intelligent houses. The stacked method is utilized to filter out the exceptions. At the same time, the tenets of the hierarchical framework completely consider the data streaming aspects in the context of intelligent homes. The precision of detection may be greatly increased in this approach. Lastly, testing findings show that the suggested approach can significantly improve efficiency while promoting communication safety in smart homes. Semi-supervised architecture and multi-categorization are utilized to increase the effectiveness of the suggested approach.

Mishra et al.[11] Identifying invasive actions within the Internet of Things, or IoT, networks is suggested using an enhanced and optimized Light Gradient Boosting Machine (LGBM) method. The main achievements are as follows: i) A more effective evolution optimization method had been used to determine the ideal LGBM extreme parameters for the proposed problem, and ii) An optimized LGBM model has been constructed to detect harmful IoT activities in the IoT network. For effective investigation of the hyper-parameter look space, a Genetic Algorithm (GA) via a k-way choice of tournaments and common overlap functioning is utilized; iii) and at last, the efficacy of the suggested approach is assessed utilising cutting-edge group learning and machine learning-driven model to attain as a whole generalized efficiency and effectiveness. The outcomes of the simulations show that the proposed methodology is better than other techniques and is an accurate method for identifying intrusions in an IoT context. Implementing IoT security

solutions in real-time utilizing the suggested method is difficult.

The IoT concept was created to improve the lives of individuals by providing a wide variety of intelligent, networked gadgets and apps across various fields. Nevertheless, safety issues are gadgets' biggest difficulties in an IoT ecosystem. IoT appliance security has been addressed in several ways, although more development is preferred. Machine learning has proven to be capable of seeing similarities when previous approaches have failed. Deep learning is one cutting-edge technique to improve IoT security. This creates a seamless solution for detecting anomalies. Saba et al.[12] Proposes a CNN-based approach for intrusion detection systems based on anomalies (IDS) that leverages the IoT's strengths and provides the ability to analyze all IoT signals efficiently. The suggested model can detect possible incursions and anomalous traffic trends. The precision of the model was 99.51 % during training and 92.85 % during testing utilizing the NID Dataset and BoT-IoT dataset. Deep learning algorithms are utilized to create various methods to enhance security protocols.

3. Problem statement

IoT technologies have gained substantial effectiveness and service quality advantages thanks to their widespread adoption across various corporate and government sectors. However, because of their inherent vulnerability and increasing spread, IoT devices are now vulnerable to serious security risks, with a particular focus on data integrity and service availability. IoT systems collect various data from various devices, making detecting anomalous behavior and compromised nodes efficiently difficult. This is in contrast to typical IT networks. Many research initiatives suggest various methods to address the urgent requirement for reliable and resilient detection of anomalies in IoT-driven systems that support decisions [13]. These strategies include deep learning-based techniques, feature selection procedures, and considering time-based anomalies while designing smart city services. Although these techniques show potential for improving IoT security, they also have implementation difficulties, resource efficiency, and practicality issues. Additionally, despite advancements in anomaly detection, the IoT still faces security issues despite its widespread usage, necessitating improved and more precise intrusion detection systems [14].

4. Proposed CNN-BiLSTM method

The suggested approach contains many essential components for maximizing the Bat-optimised CNN-BiLSTM model's ability to improve network anomaly detection in IoT scenarios. These processes involve designing the model, applying the Bat algorithms for optimization, and evaluating it using data collected from the IoT. The overall Conceptual Diagram is explained in Fig. 2.

4.1. Dataset collection

KDD99, which has been utilized in numerous research, constitutes a single dataset that is usually employed in anomaly detection. The Numenta Anomaly Benchmark (NAB) dataset, which consists of seven kinds of datasets injected with abnormalities, has also lately grown in popularity. Another publicly accessible real-world data source is Yahoo. Numerous scholars have employed additional real-world benchmark data sets that are also available. However, researchers frequently simulate real data and produce data that accurately reflects the real world when the data for specific application domains is accessible. With artificial data, researchers benefit from the data's labeling and can insert outliers or anomalies to assess how well the tools they employed for detection worked. [15].

4.2. Pre-processing

For every machine learning investigation, gathering and exploratory information analysis are required. The initial stage of the work was to convert the dataset into a classification feed. Therefore, the initial step was to deal with the missing data. Due to the transmission anomaly, the data set's "Accessed Node Type" and "Value" areas are empty. Both of these qualities are separated by the "Accessed Node Type" traits, which have categorical data, whereas the "Value" characteristics have continuous numbers [16].

There are several methods for converting data with categories into matrix. Both Labels Encoding and Single Hot Coding are widely employed. The labels encode method was used in this work to convert the information into vectors of features. Despite nominal categorization values, most of the characteristics in the data set have many unique values. If these attributes were assigned a single hot encoding, the overall number of attributes would have increased greatly, and the resulting data set might have several dimensions. However, when the encoding of labels was used, the number of characteristics remained constant. The dataset's dimension did not grow as a result. Additionally, a hot encoding value would require a lot of processing effort and thinner properties, making it more challenging to include in machine learning methods. The dataset is, therefore, submitted for labeling encoding. The main component of this pre-processing is encoding categorical data into numerical identifiers for feature representation.

4.3. Feature extraction using Bat optimization algorithm

The metaheuristic algorithm known as BA was motivated by nature. When looking for food and navigating obstacles in the pitch-black, microbats utilize an algorithm that uses their echo ability. When seeking food, microbats emit loud impulses, gradually getting quieter the farther away they are. Concepts of the micro bat's natural behavior are presented as an optimization technique to suggest BA. To determine the precise path from their current location, each bat determines its speed and position based on the exclusiveness of microbats near their target.

The following concepts concerning artificial bats attempted to organize the terms.

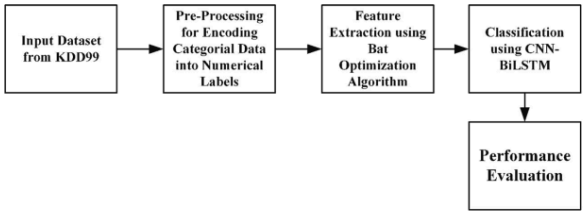


Fig. 2. Overall conceptual diagram.

1. Each micro bat uses its echo ability to gauge the distance to its environment and catch its prey.
2. In addition to different volume A_o^0 and different wavelengths, a frequency with a constant range is used to determine a micro bat's speed v_t^0 from its position x_t^0 when it is on the lookout for food.
3. When determining the distances between a food and a microbat, the emissions pulsed elements $r^0 \in [0, 1]$ may be used to modify the frequency of its pulses [17].
4. Noise will move from a significant positive value. To lower the value, A_o^0 to A_{min}^0. The four steps that make up traditional BA are as follows:

Steps:

1 Both the amount and the parameters for bats are initialized. The following is how the worldwide optimization code is written as Eq. (1)

$$\min/\max\{f_0(\dot{x})|\dot{x} \in X\} \tag{1}$$

The answer,$\dot{x_0^j} = (\dot{x_{0_1}}, \dot{x_{0_2}}, \ldots, \dot{x_{0_d}})$ with a length shown by d, is estimated using the objective functions $f_0(x)$. The BA settings are initialized using the steps listed below:

a. N_0 Represents the number of synthetic bat sites.

b. The terms $\dot{F_{0_{min}}}$ and $'$ are used to indicate the minimum and maximum frequencies, respectively.

c. The speed vector of a bat is denoted by $\dot{v_{0_j}}$.

d. $\dot{A_{0_j}}$ Represents the volume rate.

e. The symbol for pulse rate is $\dot{r_{0_j}}$.

f. $r_{0_j}^0$ Stands for a bat's first pulse rate.

g. There are two constants: α_0 and β_0.

h. £$_0$ Designates a range of bandwidth.

2. The bat population database has been set up. BM is employed for storing bat position vectors. The steps listed below are used to produce those vectors of randomness as seen in Eq. (2)

$$\dot{x_{0_i}} = \dot{LB_{0_i}} + (\dot{UB_{0_i}} - \dot{LB_{0_i}}) * (0, 1) \tag{2}$$

The answers are then stored in BM whereas the outcomes of the objective function are arranged in an ascending sequence.

$$BM = \begin{vmatrix} \dot{x_{0_1}^1} & \dot{x_{0_2}^1} \cdots & \dot{x_{0_d}^1} \\ \dot{x_{0_1}^2} & \dot{x_{0_2}^2} \cdots & \dot{x_{0_d}^2} \\ \vdots & \vdots \cdots & \vdots \\ \dot{x_{0_1}^{N_0}} & \dot{x_{0_2}^{N_0}} & \dot{x_{0_d}^{N_0}} \end{vmatrix} \tag{3}$$

3 Regrowth of the present one bat population.

Each bat's position is reconstructed using the choice, growth, and intensification operators. The intensification operator creates a new bat the spot,$\dot{x_0^j}$, as seen below in Eqs. (4)–(6)

$$\dot{F_{0_j}} = \dot{F_{0_{min}}} + \left(\dot{F_{0_{min}}} - \dot{F_{0_{max}}}\right) * (0, 1) \tag{4}$$

$$\dot{v_{0_i}} = \dot{v_{0_i}} + \left(\dot{x_{0_i}} - \dot{x_{0_i}^{Gbest}}\right) * \dot{F_{0_j}} \tag{5}$$

$$\dot{x_{0_i}^j} = \dot{x_{0_i}^j} + \dot{v_{0_i}^j} \tag{6}$$

Utilizing the diversification operator, a local search technique is employed to generate the bat's new spot. As a result, the most recent setting,$\dot{x_0^j}$, can be determined as follows in Eqs. (7), (8)

$$\dot{x_{0_i}^j} = \dot{x_{0_i}^{best}} + \in \dot{A_{0_j}} \tag{7}$$

$$\dot{x_0^j} \leftarrow \begin{Bmatrix} \dot{x_0^{best}} + \in \dot{A_{0_j}} & \dot{U(0,1)} > \dot{r_{0_j}} \\ \dot{x_{0_j}} + \dot{v_{0_j}} & otherwise \end{Bmatrix} \tag{8}$$

When using the choice operator [17], the bat's present place is changed to a new one, updating $\dot{x_0^{Gbest}}$ in the process $\dot{f\left(x_{0_j}^j\right)} < \dot{f\left(x_{0_i}^{Gbest}\right)}$ is shown in Eqs. (9), (10)

$$\dot{r_{0_j}} = \dot{r_{0_j}^0}(1 - e^{\dot{(-\gamma^*)}}) \tag{9}$$

$$\dot{A_{0_j}} = \alpha_0 \dot{A_{0_j}} \tag{10}$$

$$\dot{A_{0_j}^{in}} \to 0, \dot{r_{0_j}} \to \dot{r_{0_0}^0}, where it r \to \infty$$

4 Stopping standards.

Up till the cancellation criteria are satisfied, the earlier process is repeated. In Algorithm 1, a mock code for BA is provided.

Algorithm 1. *BA Pseudo code.*

Sensor with Rich RSSI value

```
for j = 1 to N_0 do
for i = 1tod do
x'_{0_i} = LB_{0_i} + (UB_{0_i} − LB_{0_i}) * (0, 1)
End for
End for
Calculating x_0^{Gbest}, where Gbest ∈(1, 2….N_0)
While total iterations > itr do
for j = 1 to N_0 do
F_{0_j} = F_{0_min} + (F_{0_min} − F_{0_max}) * (0, 1)
for i = 1 to d do
v'_{0_i} = v'_{0_i} + (x'_{0_i} − x'^{Gbest}_{0_i}) * F'_{0_j}
x'^j_{0_i} = x'^j_{0_i} + v'^j_{0_i}
End for
if U_0 (0, 1) > r'_{0_j} then
for i = 1 to d do
x'^j_{0_i} = x'^{best}_{0_i} + ∈ A'_{0_j}
End for
End if
If U_0 (0, 1) > A_{0_j} and f(x'^j_{0_i}) < f(x'^{Gbest}_{0_i}) then
x'^j_0 = x'^j_0
f(x'^j_0) = f(x'^j_0)
A_{0_j} = α_0 A_{0_j}
r'_{0_j} = r'^0_{0_j}(1 − e^{(−γ*)})
End if
End for
Updating x'^{Gbest}_0, Gbest ∈(1, 2…N_0)
End while
```

The presented code sample looks to be part of the pseudocode for an optimization process, most likely a Particle Swarm Optimization (PSO) variation or a closely related evolutionary optimization method. This algorithm uses N_0 particles (sensors) with d-dimensional coordinates (x) and velocity (v) and iteratively updates each particle's position according to predefined rules. It seeks to minimize a fitness function (f) and identify the best solution (Gbest). The use of random numbers $U_0(0, 1)$ to generate specific particle behaviors is one of the key components, along with randomized for exploring new positions (x), the adaption of velocities (v) based on historically optimal results (Gbest), and randomization to adapt velocity (v). The algorithm's behavior is further controlled by parameters like $\dot{F_{0_{min}}}$, $\dot{F_{0_{max}}}$, α_0, and γ^*. The Gbest and the positions of the particles in the search space are updated continuously as the algorithm runs for the predetermined number of iterations (itr). Generally speaking, it is an iterative optimization process using randomized and adaptation mechanisms to identify the best solution for the specified fitness function within the given restrictions and parameters.

4.4. Classification using CNN-BiLSTM

In the business Internet of Things, numerous data streams frequently exhibit significant localized correlations, and a few of these data points even directly correlate to data across an extended span. By employing a technique to separate the crucial information from the rest of the data, the BiLSTM neural network can successfully handle such time-sequential data. Therefore, this study incorporates the CNN-based BiLSTM network to improve the detection capabilities of the system of detection. The figure displays CNN-BiLSTM's suggested industrial IoT intrusion detection paradigm. The initial data set must be filtered in the identification model's first step. Before being standardized and normalized, all the information is converted into numerical information. The database representations layer receives the information that was processed. After preliminary processing, the record's presentation layer uses an embedded form for every bit of information [18]. The feature formula results are as follows when all the information features have been convolution-checked in Eq. (11). Fig. 3 shows the architecture of BiLSTM.

$$H_0^d = [h_1^d, h_2^d, \cdots h_{n-d_i+1}^d] \tag{11}$$

To create the characteristic sequence, all of the characteristics of H_0^d from convolution are merged and the formula is as follows in Eq. (12)

$$H_{0_v} = [h_{01}, h_{02}, \cdots h_{0n-d_i+1}] \tag{12}$$

The map of features is obtained by the convolution layer, which then passes it to the pooling layer following convolution processing. After that, the distinctive patterns are gathered in a single layer for pooling. By splitting the data set cap H sub 0 to the d into M blocks, finding the greatest value in every block, and combining the results, an eigenvector can be calculated using the greatest pooling method. The eigenvector's length is M and the outcome is given by Eq. (13)

$$P_{0_i} = [p_{m_1}, p_{m_2}, \ldots p_{m_n}] \tag{13}$$

Where P_{m_i} is a vector representation generated by the layer of pooling following a block's pooled process m_i. Fig. 4 explains the CNN-BiLSTM of IOT detection.

The acquired characteristic sequence is then entered into the BiLSTM layer following the information pooled in the pooling layer. Dual LSTM components comprise the long short-term memory layer, and various weights among them are exchanged. All information is sequentially selected and removed using the BiLSTM module. After evaluating the information, the CNN-BiLSTM network requires the data characteristics. These characteristic sequences are integrated using a full connection layer, and the full connection layer's output is fed into the softmax classifier. The outcomes for every data classification is obtained [18].

5. Results and discussion

5.1. Evaluation parameters

Various evaluation metrics will be utilized to assess the efficiency of the suggested system. Understanding the effects of various hyper-parameters evaluated on the suggested framework will be easier with the aid provided by these assessment parameters. These criteria for assessment will also make it easier to evaluate the suggested system's effectiveness compared to current systems [19].

5.1.1. Confusion matrix

The efficacy of classification on an array of test information the classification algorithm is blind to is frequently described using a confusion matrix. The confusion matrix is produced as a table that is quite easy to comprehend [20]. Fig. 7 shows the confusion matrix of this proposed method.

5.1.2. Correlation heat map

The correlation heat map is a visual tool that shows the correlation among many variables as a matrix of values with different colors [21]. Similar to a color chart, it demonstrates how closely linked various factors are shown in the Fig. 8.

Fig. 5 shows how the testing and training datasets perform, and Fig. 6 shows the training and validation model accuracy and losses. Choosing the most suitable hyper-parameter values and the system's fundamental design to construct the most effective detection system for intrusions based on deep learning algorithms is essential. Researchers experimented with several setups by changing some of the model's hyper-parameters, including 1. The Number of Layers, 2. Loss of Function 3. The number of epochs and the development of the best design.

A graph called a confusion matrix is used to describe how well a classification system performs.

5.1.3. Accuracy

The degree to which the measured value is accurate about a reference or established value. When tests for a specific object are near to a

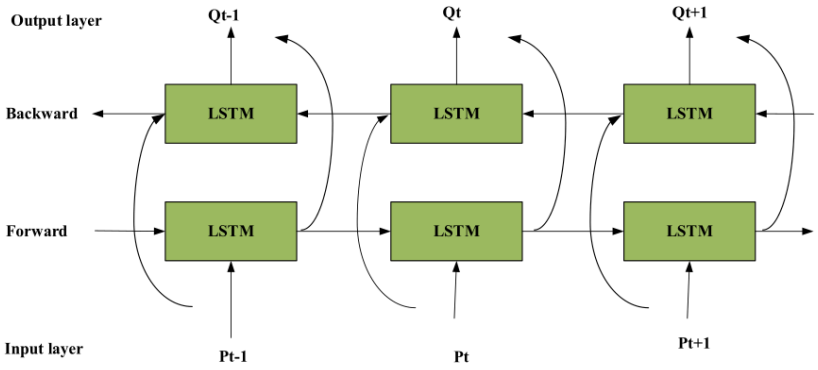


Fig. 3. BiLSTM architecture.

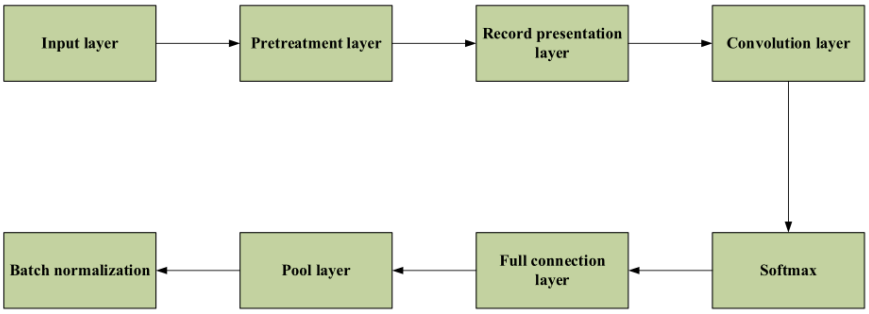


Fig. 4. Utilising CNN-BiLSTM, an Internet of Things detection.

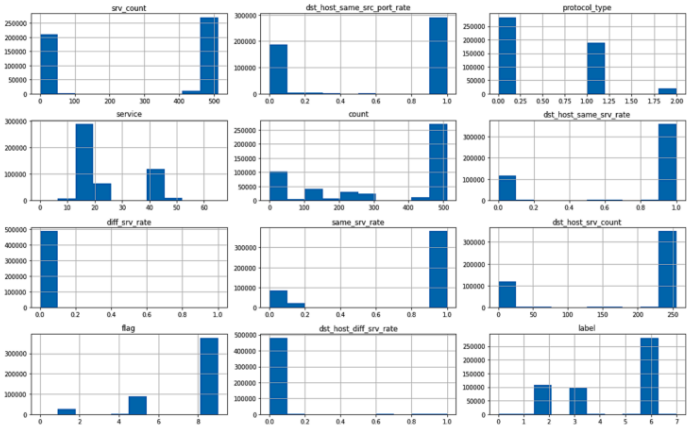


Fig. 5. Training and testing datasets.

recognized number yet widely apart from one another, it indicates the measurement's accuracy is lacking in precision. Accuracy is determined as Eq. (14).

$$Accuracy = TP + TN/TP + TN + FP + FN \tag{14}$$

5.1.4. Precision

Being accurate means being precise. Regardless of whether the measurements are correct, it describes how near two or more measures are to one another. The calculation for precision is given by Eq. (15).

$$Precision = TP/TP + FP \tag{15}$$

5.1.5. Recall

Recall is frequently employed as a fundamental performance indicator together with precision. Although recall is an estimation of quantity, accuracy measures quality. Recall is determined by Eq. (16).

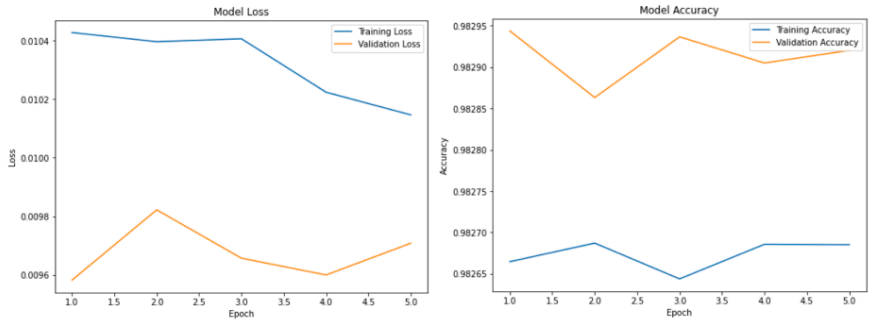
$$\text{Recall} = \text{TP} / \text{TP} + \text{FN} \tag{16}$$

5.1.6. F1 score

The F1 score, which may be viewed as a harmonic average of precision and memory, is utilized to expand on precision and recall. It could be a valuable performance indicator for unbalanced datasets [19]. F1 Score is determined by Eq. (17).

$$F1 = 2{*}TP/2{*}TP + FP + FN \tag{17}$$

The above Table. 1 and Fig. 9 shows the performance metrics such as accuracy, precision, recall, and f1 score. The proposed CNN-BiLSTM method shows higher accuracy, precision, recall, and f1 score. Three distinct classifiers, DNN, SVM, and CNN-BiLSTM, were compared regarding their performance on various tasks in the presented classification results. The performance metrics are recall, F1 score, precision, and accuracy. The CNN-BiLSTM model exhibits the greatest precision (97.35 %) among these classifiers, demonstrating its capacity to properly categorize positive cases with a low rate of false positives.



(a) (b)

Fig. 6. Training and validation Model loss and accuracy.

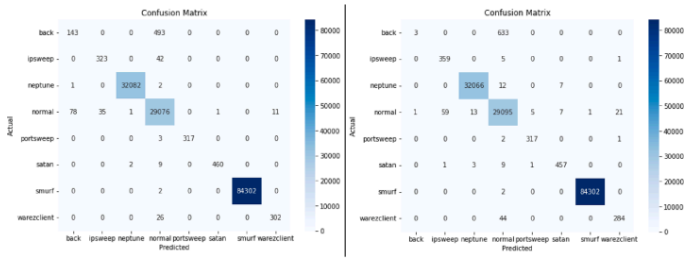
Table 1
Performance metrics of existing and proposed method [22].

Classifiers	Precision	Accuracy	F1 score	Recall
DNN	95.85	80.22	79.72	68.21
SVM	91.26	72.28	69.97	56.73
CNN-BiLSTM	97.35	99.43	85.23	83.64

Additionally, it has the greatest accuracy (99.43 %), indicating that it is often competent in correctly classifying events into positive and negative classes. The CNN-BiLSTM model has an F1 score of 85.23 %, which is noteworthy because it demonstrates a reasonable trade-off between precision and recall. With a high recollection rate of 83.64 %, this classifier can properly identify a significant fraction of positive cases. The CNN-BiLSTM model beats the DNN and SVM-based classifiers on various performance parameters, demonstrating its fit for the specific classification job. In contrast, the DNN and SVM classifiers perform almost as well.

6. Discussion

The experiment's results show that, regarding accuracy and efficiency, the Bat-optimized CNN-BiLSTM model beats cutting-edge anomaly detection methods. The model effectively recognizes a variety of computer network anomalies, such as DoS attacks, attempts at intrusion, and strange network behaviors [23,24]. This shows how successful the suggested strategy is in boosting security in IoT contexts. Incorporating the Bat method optimization increases the CNN-BiLSTM model's detecting precision. This is crucial in limited-in-resource IoT contexts with memory restrictions, processing speed, and energy use. Its performance on IoT devices influences the model's scaling and practicability. The suggested model has several advantages compared to conventional anomaly detection and current deep learning-based methods. To overcome these difficulties, the Bat optimized CNN-BiLSTM approach captures all temporal and spatial trends in IoT network activity data. Although the Bat-optimized CNN-BiLSTM approach yields positive outcomes, some restrictions must be understood. It can be difficult to conduct in-depth analyses because there may not be many practical IoT datasets with labeled network traffic data available [25]. The suggested approach has important practical implications for improving the efficiency and security of IoT systems. Organizations may proactively reduce potential risks and guarantee the dependability of IoT systems by properly identifying network irregularities. Various industries, including smart cities, factory automation,



(a) (b)

Fig. 7. Confusion matrix.

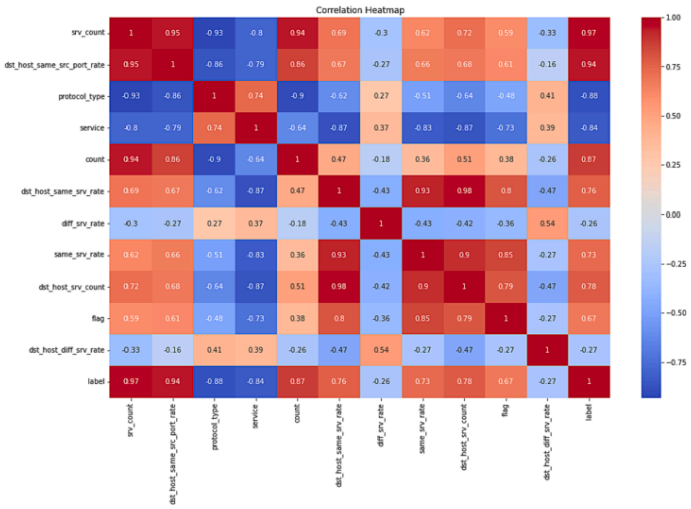


Fig. 8. Correlation heat map.

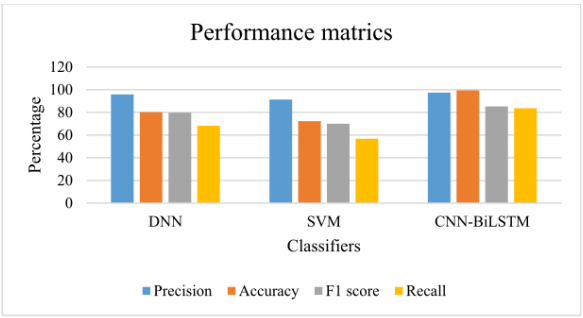


Fig. 9. Performance metrics of existing and proposed methods.

and healthcare, can use the Bat-optimised CNN-BiLSTM architecture to help build reliable and secure IoT networks.

The usefulness and benefits of the Bat-optimised CNN-BiLSTM algorithm for enhanced network detection of anomalies for Internet of Things (IoT) settings are highlighted in the talk. The model is a useful remedy due to its increased accuracy, effectiveness, and applicability for devices with limited resources. To solve potential flaws and boost performance, future studies could expand the model and investigate how it can be used in various IoT sectors.

7. Conclusion

The Bat-optimized CNN-BiLSTM framework represents a novel strategy for enhancing the security and effectiveness of IoT environments, and it is introduced in this work as a conclusion. The model successfully reflects time and space trends in IoT data by merging Convolutional Neural Networks (CNNs) for geographic analysis and Bidirectional Long Short-Term Memory (BiLSTM) systems for temporal pattern capture. By eliminating erroneous positives and false negatives, the model seeks to increase detection accuracy by utilizing the Bat method for parameter optimization. Experimental findings on IoT datasets demonstrate the model's improved performance, achieving a remarkable 99.43 % accuracy. This study offers important new knowledge about IoT anomaly detection and a promising approach to deal with the growing security issues in IoT ecosystems. The results of this study have implications for improving the overall safety record of IoT

networks and devices, protecting vital infrastructure and data across numerous industries.

Further studies could concentrate on issues such as the difficulties of internet-based and actual time anomaly detection in changing IoT networks, the practical use of the Bat-optimized CNN-BiLSTM approach to large-scale deployments of IoT, and the flexibility of the framework across different IoT domains. The Bat-optimized CNN-BiLSTM model provides a potent remedy for sophisticated network detection of anomalies in IoT applications. We can improve the safety, resiliency, and efficiency of IoT systems by harnessing the potential of deeper learning and nature-inspired optimization, opening up possibilities for trustworthy and secure IoT ecosystems across multiple industries.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Y. Li, Q. Liu, A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments, Energy Rep. 7 (2021) 8176–8186, https://doi.org/10.1016/j.egyr.2021.08.126.

[2] K. Demertzis, L. Iliadis, N. Tziritas, P. Kikiras, Anomaly detection via blockchained deep learning smart contracts in industry 4.0, Neural Comput & Applic 32 (23) (2020) 17361–17378, https://doi.org/10.1007/s00521-020-05189-8.

[3] X. Yang, G. Peng, D. Zhang, Y. Lv, An enhanced intrusion detection system for IoT networks based on deep learning and knowledge graph, Secur. Commun. Networks 2022 (2022) 1–21, https://doi.org/10.1155/2022/4748528.

[4] A. Al-Abassi, H. Karimipour, A. Dehghantanha, R.M. Parizi, An ensemble deep learning-based cyber-attack detection in industrial control system, IEEE Access 8 (2020) 83965–83973, https://doi.org/10.1109/ACCESS.2020.2992249.

[5] Z. Huang, W. Xu, K. Yu, Bidirectional LSTM-CRF Models for, Sequence Tagging (2015), https://doi.org/10.48550/ARXIV.1508.01991.

[6] A. Abusitta, G.H. de Carvalho, O.A. Wahab, T. Halabi, B.C. Fung, S. Al Mamoori, Deep learning-enabled anomaly detection for IoT systems, Internet of Things 21 (2023), 100656.

[7] M. Alanazi, A. Aljuhani, Anomaly detection for Internet of Things cyberattacks, Comput., Mater. Continua 72 (2022) 261–279, https://doi.org/10.32604/cmc.2022.024496.

[8] R. Xu, Y. Cheng, Z. Liu, Y. Xie, Y. Yang, Improved Long Short-Term Memory based anomaly detection with concept drift adaptive method for supporting IoT services, Future Gener. Comput. Syst. 112 (2020) 228–242.

[9] X. Zhou, W. Liang, S. Shimizu, J. Ma, Q. Jin, Siamese neural network based few-shot learning for anomaly detection in industrial cyber-physical systems, IEEE Trans. Industr. Inform. 17 (8) (2020) 5790–5798.

[10] Y. Cheng, Y. Xu, H. Zhong, and Y. Liu, "HS-TCN: A Semi-supervised Hierarchical Stacking Temporal Convolutional Network for Anomaly Detection in IoT," in: 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC), London, United Kingdom: IEEE, Oct. 2019, pp. 1–7. doi: 10.1109/IPCCC47392.2019.8958755.

[11] D. Mishra, B. Naik, J. Nayak, A. Souri, P.B. Dash, S. Vimal, Light gradient boosting machine with optimized hyperparameters for identification of malicious access in IoT network, Digital Commun. Networks 9 (1) (2023) 125–137.

[12] T. Saba, A. Rehman, T. Sadad, H. Kolivand, S.A. Bahaj, Anomaly-based intrusion detection system for IoT networks through deep learning model, Comput. Electr. Eng. 99 (2022), 107810, https://doi.org/10.1016/j.compeleceng.2022.107810.

[13] B. Ghimire, D.B. Rawat, Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things, IEEE Internet of Things J. 9 (11) (2022) 8229–8249.

[14] "Network intrusion detection system for DDoS attacks in ICS using deep autoencoders | SpringerLink." https://link.springer.com/article/10.1007/s11276-022-03214-3 (accessed Jul. 07, 2023).

[15] R. Al-amri, R.K. Murugesan, M. Man, A.F. Abdulateef, M.A. Al-Sharafi, A. A. Alkahtani, A review of machine learning and deep learning techniques for anomaly detection in IoT Data, Appl. Sci. 11 (12) (2021) 5320, https://doi.org/10.3390/app11125320.

[16] M. Hasan, Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches, Internet of Things (2019).

[17] A. Alharbi, W. Alosaimi, H. Alyami, H.T. Rauf, R. Damaševičius, Botnet attack detection using local global best bat algorithm for industrial Internet of Things, Electronics 10 (11) (2021) 1341, https://doi.org/10.3390/electronics10111341.

[18] A. Li, S. Yi, Intelligent intrusion detection method of industrial Internet of Things Based on CNN-BiLSTM, Secur. Commun. Networks 2022 (Apr. 2022) 1–8, https://doi.org/10.1155/2022/5448647.

[19] Y. Guan, "ACS-IoT: A CNN-BiLSTM Model for Anomaly Classification in IoT Networks".

[20] N.K. Sahu, I. Mukherjee, "Machine learning based anomaly detection for IoT network:(Anomaly detection in IoT network)," in: 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), IEEE, 2020, pp. 787–794.

[21] M. Fahim, A. Sillitti, Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review, IEEE Access 7 (2019) 81664–81681.

[22] T. Hou, H. Xing, X. Liang, X. Su, Z. Wang, A Marine Hydrographic Station Networks Intrusion Detection Method Based on LCVAE and CNN-BiLSTM, JMSE 11 (1) (2023) 221, https://doi.org/10.3390/jmse11010221.

[23] K.C. Ravikumar, N. Pandi Chiranjeevi, M. Devarajan, C. Kaur, A.I. Taloba, Challenges in Internet of things towards the security using deep learning techniques, Measurement: Sensors 24 (2022), 100473.

[24] Rasha M. Abd El-Aziz, A.I. Taloba, F.H.A. Alghamdi. "Quantum computing Optimization technique for IoT platform using the modified deep residual approach, Alexandria Eng." J 61, no. 12 (2022): 12497-12509.

[25] Saif Alghawli, Abed, Ahmed I. Taloba, An enhanced ant colony optimization mechanism for the classification of depressive disorders, Comput. Intell. Neurosci. 2022 (2022).

Unleashing the power of Bat optimized CNN-BiLSTM model for advanced network anomaly detection: Enhancing security and performance in IoT environments

ORIGINALITY REPORT

14%	%	13%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Abdullah Alharbi, Wael Alosaimi, Hashem Alyami, Hafiz Tayyab Rauf, Robertas Damaševičius. "Botnet Attack Detection Using Local Global Best Bat Algorithm for Industrial Internet of Things", Electronics, 2021 Publication	2%
2	Submitted to University College London Student Paper	1%
3	M. Veera Brahmam, S. Gopikrishnan. "RETRACTED: Adaptive threshold based outlier detection on IoT sensor data: A node-level perspective", Alexandria Engineering Journal, 2024 Publication	1%
4	Xiaojie Xu, Hui Xu, Kai Mei, Lianghuai Tong, Zhenjie Liu, Tingting Wang, Kai Fang. "Integrating multi-modal data into transformer model for short-term gas consumption forecasting", Alexandria Engineering Journal, 2025 Publication	1%
5	Pushpa Choudhary, Sambit Satpathy, Arvind Dagur, Dhirendra Kumar Shukla. "Recent Trends in Intelligent Computing and Communication", CRC Press, 2025 Publication	1%
6	Hao Ding, Qing Li, Can Wang, Hongmei Ren, Jiasi Li, Xuefeng Piao, Huihui Song, Zhenzhou Ji. "How Far Should We Go Away from Smart	<1%

Contract to Smarter Contractor? A Systematic Review", Blockchain: Research and Applications, 2025
Publication

7	Submitted to University of North Texas Student Paper	<1 %
8	"Applications of Computational Intelligence in Management and Mathematics I", Springer Science and Business Media LLC, 2025 Publication	<1 %
9	Xiaokang Zhou, Wei Liang, Shohei Shimizu, Jianhua Ma, Qun Jin. "Siamese Neural Network Based Few-Shot Learning for Anomaly Detection in Industrial Cyber-Physical Systems", IEEE Transactions on Industrial Informatics, 2021 Publication	<1 %
10	Redhwan Al-amri, Raja Kumar Murugesan, Mustafa Man, Alaa Fareed Abdulateef, Mohammed A. Al-Sharafi, Ammar Ahmed Alkahtani. "A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data", Applied Sciences, 2021 Publication	<1 %
11	"Advanced Intelligent Computing Technology and Applications", Springer Science and Business Media LLC, 2024 Publication	<1 %
12	Maryam Gallab, Mario Di Nardo, Lina Naciri. "Navigating contemporary challenges and future prospects in digital industry evolution", Discover Applied Sciences, 2024 Publication	<1 %
13	Taviti Naidu Gongada, Amit Agnihotri, Kathari Santosh, Vijayalakshmi Ponnuswamy et al. "Leveraging Machine Learning for Enhanced Cyber Attack Detection and Defence in Big	<1 %

Data Management and Process Mining", International Journal of Advanced Computer Science and Applications, 2024
Publication

14	Mahmudul Hasan, Md. Milon Islam, Md Ishrak Islam Zarif, M.M.A. Hashem. "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches", Internet of Things, 2019 Publication	<1 %
15	Divya Nimma, Omaia Al-Omari, Rahul Pradhan, Zoirov Ulmas, R.V.V. Krishna, Ts. Yousef A.Baker El-Ebiary, Vuda Sreenivasa Rao. "Object detection in real-time video surveillance using attention based transformer-YOLOv8 model", Alexandria Engineering Journal, 2025 Publication	<1 %
16	Submitted to Higher Education Commission Pakistan Student Paper	<1 %
17	C. Jackulin, S. Murugavalli, K. Valarmathi. "RIFATA: Remora improved invasive feedback artificial tree algorithm-enabled hybrid deep learning approach for root disease classification", Biomedical Signal Processing and Control, 2023 Publication	<1 %
18	Adel Abusitta, Glaucio H.S. de Carvalho, Omar Abdel Wahab, Talal Halabi, Benjamin C.M. Fung, Saja Al Mamoori. "Deep learning-enabled anomaly detection for IoT systems", Internet of Things, 2023 Publication	<1 %
19	"Intelligent Technologies", Springer Science and Business Media LLC, 2024 Publication	<1 %

20	Afnan M. Alhassan. "Versa net fusion with hybrid feature selection for intrusion detection in IoT", Journal of Engineering Research, 2025 Publication	<1 %
21	Ameer El-Sayed, Ahmed A. Toony, Fayez Alqahtani, Yasser Alginahi, Wael Said. "CO-STOP: A Robust P4-Powered Adaptive Framework for Comprehensive Detection and Mitigation of Coordinated and Multi-Faceted Attacks in SD-IoT Networks", Computers & Security, 2025 Publication	<1 %
22	Debasmita Mishra, Bighnaraj Naik, Janmenjoy Nayak, Alireza Souri, Pandit Byomakesha Dash, S. Vimal. "Light gradient boosting machine with optimized hyperparameters for identification of malicious access in IoT network", Digital Communications and Networks, 2022 Publication	<1 %
23	Dubey, Shiv Ram, and Anand Singh Jalal. "Species and variety detection of fruits and vegetables from images", International Journal of Applied Pattern Recognition, 2013. Publication	<1 %
24	Franciskus Antonius Alijoyo, Taviti Naidu Gongada, Chamandeep Kaur, N. Mageswari et al. "Advanced hybrid CNN-Bi-LSTM model augmented with GA and FFO for enhanced cyclone intensity forecasting", Alexandria Engineering Journal, 2024 Publication	<1 %
25	Aichuan Li, Shujuan Yi. "Intelligent Intrusion Detection Method of Industrial Internet of Things Based on CNN-BiLSTM", Security and Communication Networks, 2022 Publication	<1 %

26	Mohammad Rostamzadeh-Renani, Mohammadreza Baghoolizadeh, S. Mohammad Sajadi, Reza Rostamzadeh-Renani et al. "A multi-objective and CFD based optimization of roof-flap geometry and position for simultaneous drag and lift reduction", Propulsion and Power Research, 2024 Publication	<1 %
27	Yixuan Wu, Laisen Nie, Shupeng Wang, Zhaolong Ning, Shengtao Li. "Intelligent Intrusion Detection for Internet of Things Security: A Deep Convolutional Generative Adversarial Network-enabled Approach", IEEE Internet of Things Journal, 2021 Publication	<1 %
28	Chithaluri, Suryapunith. "Advancements and Challenges in the Intersection of Machine Learning and IoT Security", Southern Illinois University at Carbondale, 2024 Publication	<1 %
29	Rahul Kumar Chaurasiya, Varun Bajaj, Vishakha Chourasia. "Artificial Intelligence-based Signal Processing for Brain Activity Analysis", CRC Press, 2025 Publication	<1 %
30	S. Prasad Jones Christydass, Nurhayati Nurhayati, S. Kannadhasan. "Hybrid and Advanced Technologies", CRC Press, 2025 Publication	<1 %
31	Santosh Reddy P, Tarunika Chaudhari, Sanjiv Rao Godla, Janjhyam Venkata Naga Ramesh et al. "AI-Driven Transformer Frameworks for Real-Time Anomaly Detection in Network Systems", International Journal of Advanced Computer Science and Applications, 2025 Publication	<1 %

32	Shahid Allah Bakhsh, Muhammad Almas Khan, Fawad Ahmed, Mohammed S. Alshehri, Hisham Ali, Jawad Ahmad. "Enhancing IoT network security through deep learning-powered Intrusion Detection System", Internet of Things, 2023 Publication	<1 %
33	Zhiyong Zou, Dongyu Yuan, Qingsong Wu, Yuchen Xiao et al. "The comprehensive index for assessing the freshness of salmon using hyperspectral imaging technology combined with multisource data fusion method", Journal of Food Composition and Analysis, 2025 Publication	<1 %
34	Advances in Intelligent Systems and Computing, 2016. Publication	<1 %
35	Emanuel Krzysztoń, Izabela Rojek, Dariusz Mikołajewski. "A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study", Applied Sciences, 2024 Publication	<1 %
36	Gyan Prakash, Amandeep Kaur. "AI and Sustainable Transformations", CRC Press, 2025 Publication	<1 %
37	Mukul Kumar Gupta, Abhinav Sharma, Vinay Rishiwal, C S Meera. "Technology Developments in Computer Intelligence and their Applications in the Era of Industry 5.0", CRC Press, 2025 Publication	<1 %
38	Shakeel Ahmad, Muhammad Zubair Asghar, Fahad Mazaed Alotaibi, Yasir D. Alotaibi. "Diagnosis of cardiovascular disease using	<1 %

deep learning technique", Soft Computing, 2022
Publication

39	Suman Lata Tripathi, Om Prakash Kumar, Allwin Devaraj Stalin, Tanweer Ali. "Innovations in Computer Vision, Communication Systems, and Computational Intelligence - Proceedings of the First International Conference on Computer Vision, Communication System and Computational Intelligence (CVCNCE 2025), 08–09 May 2025, Tirunelveli, India", CRC Press, 2025 Publication	<1 %
40	Vandana Mohindru Sood, Yashwant Singh, Bharat Bhargava, Sushil Kumar Narang. "Intelligent Security Solutions for Cyber-Physical Systems", CRC Press, 2024 Publication	<1 %
41	Wengang Ma, Liang Ma, Kehong Li, Jin Guo. "Few-shot IoT attack detection based on SSDSAE and adaptive loss weighted meta residual network", Information Fusion, 2023 Publication	<1 %
42	Attarha, Shadi. "A Framework for Sensor Fault Detection and Management in Low-Power IoT Edge Devices", Universitaet Bremen (Germany) Publication	<1 %
43	Sehar Zehra, Ummay Faseeha, Hassan Jamil Syed, Fahad Samad, Ashraf Osman Ibrahim, Anas W. Abulfaraj, Wamda Nagmeldin. "Machine Learning-Based Anomaly Detection in NFV: A Comprehensive Survey", Sensors, 2023 Publication	<1 %
44	Harahsheh, Khawlah. "Enhancing IoT Security Using Lightweight Machine Learning	<1 %

Algorithms: A Comprehensive Approach Using Ensemble Learning, Feature Selection, and Federated Transfer Learning", Old Dominion University, 2025
Publication

45 Seyed Salar Sefati, Bahman Arasteh, Simona Halunga, Octavian Fratu. "A comprehensive survey of cybersecurity techniques based on quality of service (QoS) on the Internet of Things (IoT)", Cluster Computing, 2025 <1%
Publication

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		