Int. j. inf. tecnol.
https://doi.org/10.1007/s41870-025-02576-z

ORIGINAL RESEARCH

Blockchain-enabled cybersecurity for IoT using elliptic curve cryptography and black winged kite model

Priyanka Pramod Pawar[1] · F. Fanax Femy[2] · N. Rajkumar[3] · S. Jeevitha[4] · A. Bhuvanesh[5] · Deepak Kumar[1]

Received: 26 January 2025 / Accepted: 28 April 2025

Abstract Because of features like security, immutability, and decentralization, blockchain (BC) is important to cybersecurity. The development of Internet of Things (IoT) networks has created serious cybersecurity issues and necessitated the use of cutting-edge defenses against new dangers. Multi-Head Attention Bidirectional Long Short Term Memory (MHA-BiLSTM), a Deep Learning (DL) technique, is presented in this paper to improve cybersecurity in an Internet of Things setting. This work includes steps like data storage, encryption, decryption, and cyberattack detection. First, Elliptical Curve Cryptography (ECC) is used to encrypt the data, and Black-Winged Kite (BWK) optimization is used to optimize the ECC's key parameters. The data is stored in the BC following the encryption process. The data is then decrypted using ECC, and the MHA-Bi-LSTM completes the cybersecurity procedure. This model improves its ability to recognize and lessen cyberthreats. The proposed cybersecurity model significantly improved threat detection accuracy, according to analysis. This method offers a scalable, resilient, and cyberattack-proof model for securing IoT networks in real-time applications.

✉ Priyanka Pramod Pawar
pripawar7@gmail.com

[1] Department of Information Technology, University of the Cumberlands, Williamsburg, USA

[2] Department of Computer Science, Holy Cross College (Autonomous), Nagercoil, Tamil Nadu, India

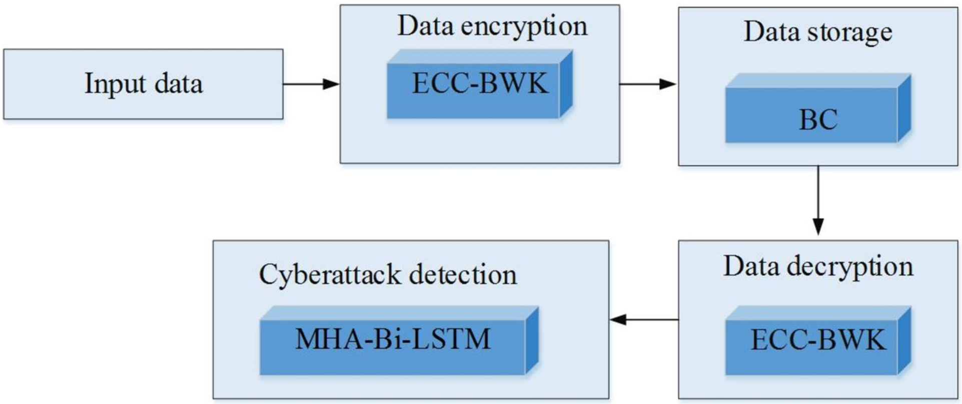
[3] Department of Computer Science and Engineering, Vel Tech Rangarajan Dr, Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India

[4] Department of Computer Science and Information Technology, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India

[5] Department of Electrical and Electronics Engineering, PSN College of Engineering and Technology, Tirunelveli, Tamil Nadu, India

Published online: 16 May 2025

Graphical abstract



Keywords Blockchain · Cybersecurity · Cyberattacks · Deep learning · Enhanced black-winged kite

1 Introduction

With the growing reliance on cloud technologies in modern society, combined with the fundamental human requirement to communicate and exchange data through digital networks, Internet of Things (IoT) devices play a crucial role in modern business operations [1]. The exchange of social and transactional data for instance financial markets accelerates the rapid advancement of emerging technologies to meet the ever-growing supply and demand dynamics [2]. In household environments, sharing digital media, like images, videos, music, and documents, through messaging platforms enhances fields such as information technology, social sciences, sports, healthcare and education, IoT devices facilitate the perfect and instant global transfer of this data via the cloud, through the Internet of Everything (IoE) [3].

Cybersecurity is implementing measures for safeguard computer systems, data, and networks from disruptions, unauthorized access, use, modification, disclosure, and destruction [4]. Thus, understanding cybersecurity and its applications for IoT and smart devices raises additional questions that require examination via different concepts of cyberspace. One of the various methods for standardizing the different terminologies, like focusing the requirement for understanding the nature of network intrusions, detection methods, and strategies for preventing cyber threats [5]. In terms of prevention, a combination of Artificial Intelligence (AI) and Machine Learning (ML) can play an important role in enhancing data security and protection.

Blockchain (BC) is frequently mentioned as Distributed Ledger Technologies (DLT) used to maintain the data storage integrity and exchange in environments that lack centralized trust [6]. It operates as a Peer-to-Peer (P2P) decentralized system, allowing secure data exchanges between untrusted participants within a network. BC systems like Hyperledger and Ethereum obtained extensive foundational frameworks, for various BC-related software applications [7]. Key attributes of BC, like decentralization and stability, are highly valued by industries like finance and healthcare for magnifying their operational efficiency [8]. BC can reduce different cyber threats by ensuring data integrity, and strengthening trust among devices. Its decentralized nature minimizes the risk of a single point of failure, a common susceptibility in existing centralized systems [9].

In IoT, combining Deep Learning (DL) with BC technology increases cybersecurity. DL models can identify complex patterns in large data and making them highly powerful in identifying abnormality and cyber threats in real-time [10]. When integrating DL with BC, these models benefit from secure data inputs. This increases the accuracy and reliability of cyberattack detection. Thus, DL with BC improves threat detection and facilitates secure data sharing and association over networks. This provides the way for more robust and adaptive IoT security frameworks [11]. The contributions are:

- To introduce the ECC-BWK algorithm for enhancing the encryption and decryption process and reducing computational overhead.
- To present the DL model MHA-Bi-LSTM for advanced threat detection capabilities by accurately identifying and classifying cyberattacks.

- By integrating BC, the system provided decentralized data storage and protects from unauthorized access.

2 Related works

Nguyen et al. [12] utilized sensor devices for data collection and employ a Deep Belief Network (DBN) for detecting intrusions. Then, it incorporated a Multiple Share Creation (MSC) approach to generate different shares of the obtained images, enhancing security and privacy. Here, the BC ensured secure data transmission and the ResNet was used for identifying the disease presence.

Rathore et al. [13] suggested model DeepBlockIoTNet integrated with BC for IoT networks, and offered significant advancements in DL for big data analysis. The framework provides three key contributions: It introduced a Distributed DL (DDL) model which facilitated DL operations at the edge layer which helps address limitations associated with performing DL at the cloud layer. This DDL was implemented within a BC and addresses key limitations in edge intelligence. At last, the DeepBlockIoTNet was validated through experimental evaluation.

Unal et al. [14] presented the cyber situational awareness engine facilitates alert segregation using an entropy weighted power k-means clustering. Here, the weights were dynamically updated through the Adaptive Transit Search (ATS). Then, the hybrid model Soergel with Lorentzian was used for selecting features and finally, the Deep Maxout Network (DMN) was used for predicting intrusion alerts. Based on the prediction outcomes, cyberattack mitigation was performed by implementing a blacklist mechanism for enhancing system security.

Kumar et al. [15] presented Digital Twin (DT) based Software-Defined Networking (SDN) for smart grid. Here, Bidirectional-Gated Recurrent Unit (Bi-GRU) was used for cyberattack detection and softmax was used for enhancing attack identification model. DT method was ultimately incorporated into the SDN control plane. This integration allows the control plane for storing behavioral method and operational phase of Smart Machines and facilitating communication with them.

Veeramakali et al. [16] introduces an IoT and healthcare diagnostic approach which considered an optimal Deep Neural Network (DNN) based secure BC. The stages like secure transaction management, encrypting hash value, and medical diagnosis. Here, the optimal process was performed by the Orthogonal Particle Swarm Optimizer (OPSO). The Neighborhood Indexing Sequence (NIS) was used for hash value. At last, the DNN with OPSO was employed as a classifier for diagnose diseases.

Unal et al. [14] suggested Federated Learning (FL) based BC for securing big data analytics. By the integration of the FL with BC provided better integrity and overcome poison attacks. For protecting the user data security and the trained approaches, the fuzzy hash was utilized and the performance was carried out over poison attacks.

3 Proposed model

In this work, cybersecurity involves a multi-stage approach to ensure data security and integrity in IoT environments. Initially, data is encrypted using ECC-BWK algorithm and provides better secure encryption. Further, it ensures confidentiality and protection from unauthorized access. After the process of encryption, the data is stored on a BC and it offers secure and transparent data communication in IoT. After retrieval, the data is decrypted using ECC-BWK, restoring it to its original form. The MHA-Bi-LSTM model then performs the cybersecurity process. This model detects cyber threats by analyzing the decrypted data. The suggested model provided enhances security by ensuring data protection and better detection of cyberattacks in IoT systems. Figure 1 shows the framework of the suggested cybersecurity process.

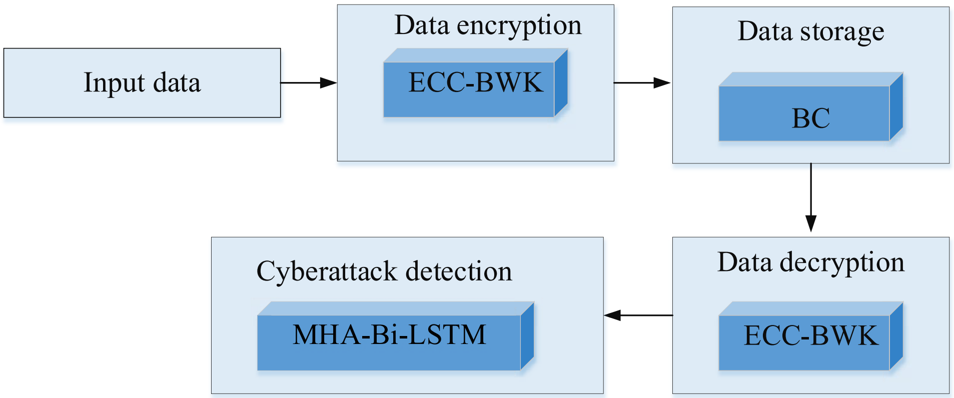


Fig. 1 Framework of suggested cybersecurity process

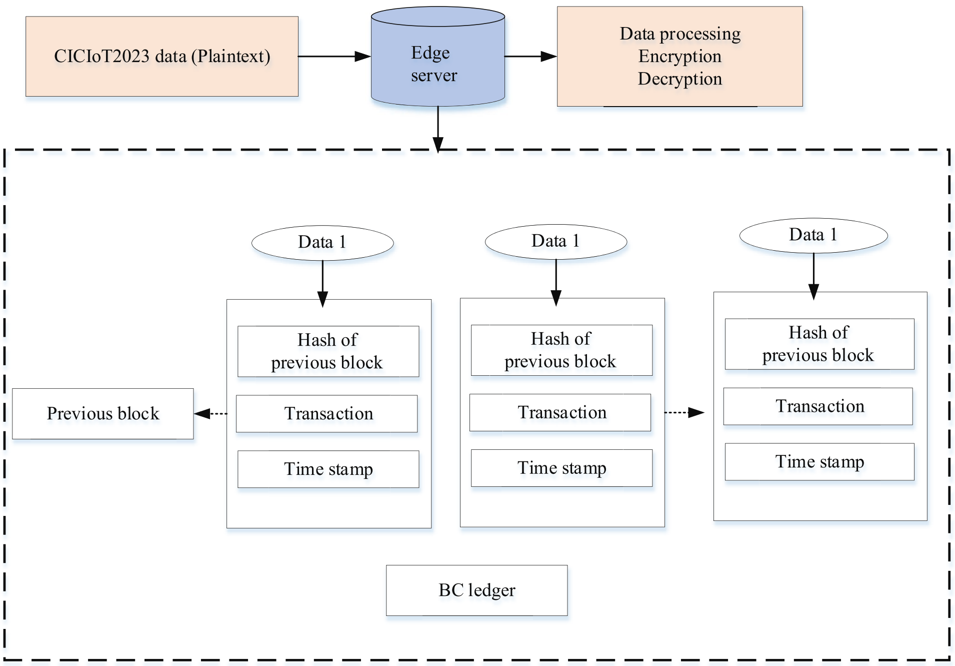


Fig. 2 Data processing in BC

3.1 Dataset acquisition

The dataset CICIoT2023 [17] was introduced in 2023 by Canadian Institute for Cybersecurity (CIC). The data offers a comprehensive resource for studying IoT based cyberattacks. This data captures a variety of malicious activities performed by compromised IoT devices targeting other IoT systems. The data has 232,885 network connections and encompasses 47 various features. The dataset covers 33 specific sub-attacks and grouped into 7 main categories: Denial of Service (DoS), Distributed DoS (DDoS), web based attacks, reconnaissance, Mirai, brute-force attacks, and spoofing.

3.2 Encryption

The input data CICIoT2023 is encrypted using ECC and it has benefits like small key size, low computational overhead and provides security when compared to conventional public key protocols. Based on mathematical model of elliptic curves, EE provides better communication among two nodes via key exchange and provides data integrity. In ECC, the points on the elliptic curve are stated as:

$$a^2 \bmod g = f^3 + g \times f \times l \bmod g \tag{1}$$

where a, f is the set of points g, l is the elliptic curve vertices.

Let two points A and B on elliptic curve U, the basic group operation has point addition, point subtraction, point doubling, and scalar multiplication.

Point addition is given as:

$$A + B = J \tag{2}$$

where J is used for connecting A and B intersect the curve.

Point subtraction is given as:

$$A - B = A + (-B) \tag{3}$$

Point doubling is given as:

$$A + A = 2A = S \tag{4}$$

where A result in the new point S.

Scalar multiplication is given as:

$$A + A + \cdots + A = kA \tag{5}$$

where k is the value of the scalar.

To further strengthen the system, an optimization algorithm BWK is applied to fine-tune the key parameters of ECC, optimizing encryption and decryption performance. This provides faster processing and reduced resource consumption. It is critical for IoT devices with less computational power.

The BKA is inspired by the hunting and migratory behaviors of the Black-winged Kite (BK), and specifically modeling its attack strategies and migration patterns. Figure 2 presents the pseudocode for the BKA and it shows the operational flow. The stages like initialization, attacking strategy, migratory strategy and balancing-diversity analysis.

Initialization: In BKA, the initial step involves generating a collection of random solutions for forming the population. Each solution, representing the position of an individual BK and it is present in a matrix format as follows:

$$BK = \begin{bmatrix} BK_{1,1} & BK_{1,2} & \cdots & BK_{1,d} \\ BK_{1,1} & BK_{1,2} & \cdots & BK_{1,d} \\ \vdots & \vdots \ \vdots & & \vdots \\ BK_{q,1} & BK_{q,2} & \cdots & BK_{q,d} \end{bmatrix} \tag{6}$$

where d is the dimension is the size of the population, BK_{lm} is the m^{th} dimension of the l^{th} BK. Every BK position is uniformly given as:

$$Z_l = BK_{lb} + r \times \left(BK_{ub} - BK_{lb}\right) \tag{7}$$

where r, BK_{ub} and BK_{lb} are the random number, upper bound and lower bound.

During the initialization phase of the BKA, the individual with the large value of the fitness in the initial population is chosen as the header Z_H. This Z_H represents the best position among the BK. The Z_H can be mathematically expressed, using the minimum fitness value and it is given as:

$$f_b = \min imum\left(f\left(Z_l\right)\right) \tag{8}$$

$$Z_H = Z\left(find\left(f_b == f\left(Z_l\right)\right)\right) \tag{9}$$

Attacking strategy: BK, known for preying on tiny insects grassland and, mammals and adapt their tail and wing angles on the basis of the wind speed when it flies. They silently hover in place to monitor their prey before swiftly diving down to capture it. This process has various attacking characteristics for global exploration and search. This strategy is expressed as:

$$x_{t+1}^{l,m} = \begin{cases} x_t^{l,m} + i(1 + \sin(r)) \times x_t^{l,m} & s < r \\ x_t^{l,m} + i(2r - 1) \times x_t^{l,m} & elsewhere \end{cases} \tag{10}$$

$$i = 0.05 \times \exp\left(2 \times (t/T)\right) \tag{11}$$

where T is the overall iterations, $x_t^{l,m}$ and $x_{t+1}^{l,m}$ are the position of the m^{th} dimension of the l^{th} BK at t and $t+1$ iterations. The value of s is 0.9 and it is a constant number.

Migratory strategy: Migration behaviour of the birds is influenced by environmental factors like food availability and climate. In the context of the BKA, if the current population's fitness value is less than the randomly generated population, the header renounces its role and joins the migrating group. This indicates its unsuitability for guiding the population forwarding process. Conversely, when the current population's fitness value higher than the randomized population, the header continues to direct the set toward its target. This mechanism ensures that only the most capable headers are selected dynamically and enhancing the chances of a better relocation. This process is given as:

$$x_{t+1}^{l,m} = \begin{cases} x_t^{l,m} + B(0,1) \times \left(x_t^{l,m} - H_t^m\right) & F_l < F_{rl} \\ x_t^{l,m} + B(0,1) \times \left(H_t^m - n \times x_t^{l,m}\right) & elsewhere \end{cases} \tag{12}$$

$$n = 2 \times \sin\left(r + \pi/2\right) \tag{13}$$

where H_t^m is the header score of the BK position of the m^{th} dimension at t. F_l is the present position, F_{rl} is the random position and $B(0,1)$ is the Cauchy mutation. The one dimension Cauchy distribution is a continual probability of distribution with dual parameter. The below expression is used for defining Cauchy distribution:

$$f(y, \alpha, \gamma) = \frac{1}{\pi} \frac{\alpha}{\alpha^2 + (y - \gamma)^2} \qquad -\infty < y < \infty \tag{14}$$

where $\gamma = 0$ and $\alpha = 1$.

```
**Input:** Size of the population, BK, iterations and dimension
**Output:** Optimal value
Compute every BK's fitness
    while $t < T$ do
Attacking strategy
        when $s < r$
            $x_t^{l,m} + i(1 + \sin(r)) \times x_t^{l,m}$
    else
            $x_t^{l,m} + i(2r - 1) \times x_t^{l,m}$
    end if
Migratory strategy
        when $F_l < F_{rl}$
            $x_t^{l,m} + B(0,1) \times \left(x_t^{l,m} - H_t^m\right)$
    else
            $x_t^{l,m} + B(0,1) \times \left(H_t^m - n \times x_t^{l,m}\right)$
    end if
Choose the best individual
End while
Return Optimal value
```

3.3 Data storage

The encrypted data from ECC is stored in blockchain (BC) and it shows the process of establishing a connection and adding new blocks to the previous block. For initiating the connection, a member, which could be any authenticated person in the cybersecurity model, sends a message

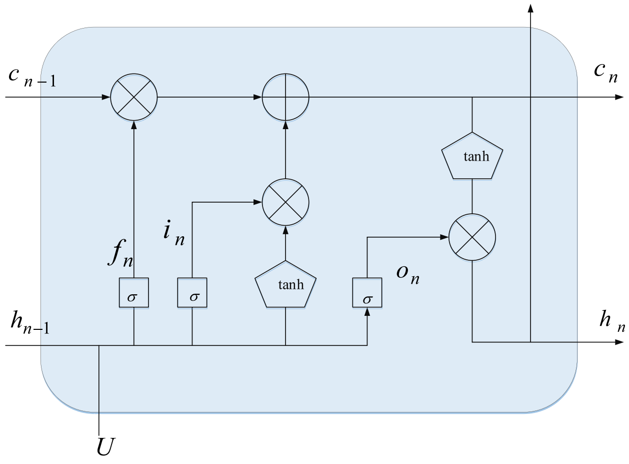


Fig. 3 Structure of the LSTM

indicating the creation of a new block or record. This newly created block may have different information, all of which are distributed across the network devices via the BC. The transaction is stored within the block and shared with all network nodes. Once the BC is completed, all nodes in the network hold an identical copy of the data and makes members to join during the verification process. They confirm the integrity of the block containing the transactions as soon as it is send to the network participants. After successful verification, the new block is added to the previous block. Each block in the BC contains three elements: data, the hash of the current block, and the hash of the previous block. The authenticated person can decrypt the data using ECC. Figure 2 shows the data processing in BC.

3.4 Cyber attack detection

The decrypted data is fed to the MHA-Bi-LSTM for Cyber attack detection. The LSTM network share a fundamental framework with general Recurrent Neural Networks (RNN) but employ a distinct approach for computing hidden states. This design addresses the challenge in RNN in managing long-term dependencies. The superior performance of LSTM models is not simply due to algorithmic learning but is attributed to their specialized structural design. Each LSTM unit has multiple repeating memory blocks and each containing three essential gates as shown in Fig. 3.

Let the input data U, the state values in the LSTM is defined as:

The forget gate f_n at time n shows which prior information must be kept and the sigmoid function σ controls the output of the gate.

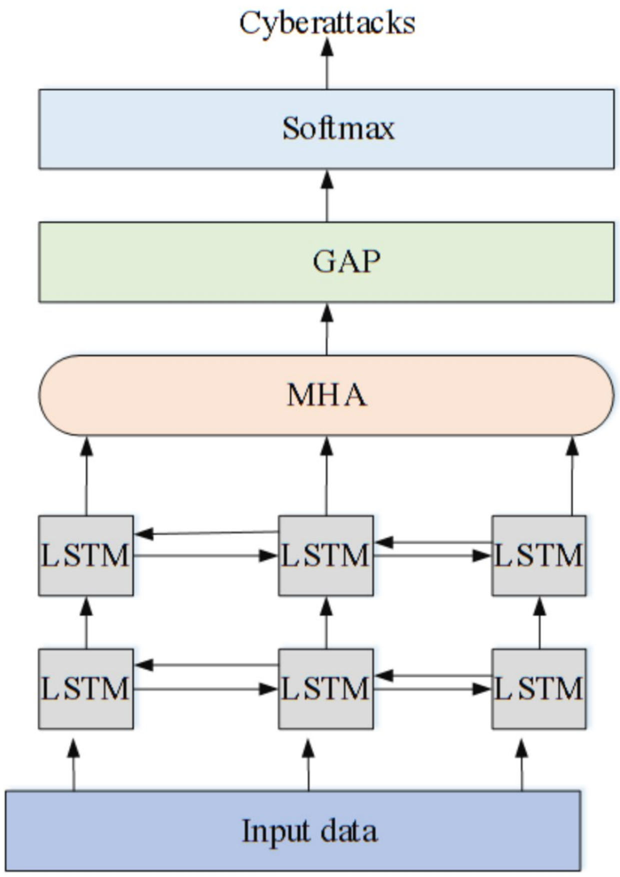


Fig. 4 Structure of the MHA-Bi-LSTM

$$f_n = \sigma\left(W_f + V_f h_{n-1} + b_f\right) \tag{15}$$

The input gate i_n shows the impacts of the input on the memory cell state c_n and it also uses σ.

$$i_n = \sigma\left(W_i + V_i h_{n-1} + b_i\right) \tag{16}$$

The candidate's memory cell $\tilde{c}_n$ shows the potential new information and it uses activation function tanh.

$$\tilde{c}_n = \tanh\left(W_c + V_c h_{n-1} + b_c\right) \tag{17}$$

The memory cell state c_n combines new information and keeps prior information c_{n-1}.

$$c_n = i_n \circ \tilde{c}_n + f_n \circ c_{n-1} \tag{18}$$

Output gate o_n shows the output from the present memory state.

$$\tilde{c}_n = \tanh\left(W_c + V_c h_{n-1} + b_c\right) \tag{19}$$

The hidden state is computed by integrating activation of the o_n with c_n.

$$h_n = o_n \circ \tanh\left(c_n\right) \tag{20}$$

The standard LSTM models process sequences based solely on historical information, Bidirectional LSTM (Bi-LSTM) enhance performance by considering both past and future contexts. A Bi-LSTM consists of two layers: a forward LSTM layer, which processes data from past to future, and a backward LSTM layer, which processes data in the reverse order. Both layers feed into the same output layer and enhance the feature extraction process. The forward hidden state $\overrightarrow{h_n}$ at time n is given as:

$$\overrightarrow{h_n} = L\left(\overrightarrow{h_n - }1, c_n - 1\right) \tag{21}$$

The backward hidden state $\overleftarrow{h_n}$ at time n is given as:

$$\overleftarrow{h_n} = L\left(\overleftarrow{h_n - }1, c_n - 1\right) \tag{22}$$

These two hidden states are combined to get h_n as:

$$h_n = \overrightarrow{h_n} \oplus \overleftarrow{h_n} \tag{23}$$

where $\oplus$ is the concatenation.

MHA: This layer adds another layer of flexibility and enables the model to prioritize specific parts of the sequence that are more relevant to the current output. For every MHA, the queries Q, keys K and values V. Figure 4 shows the structure of the MHA-Bi-LSTM For the single attention head, the attention At is computed as:

$$At(Q, K, V) = soft\max\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{24}$$

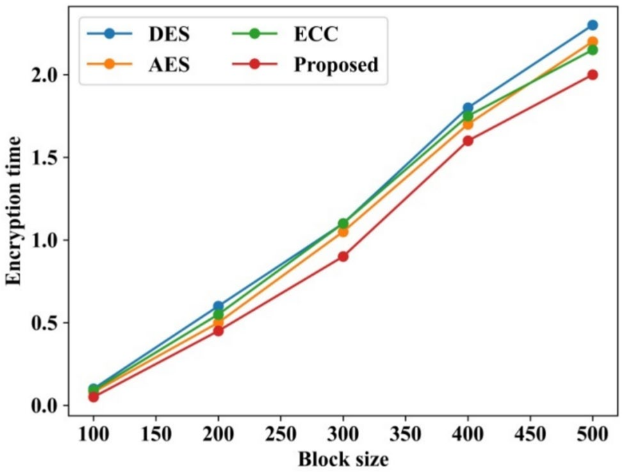


Fig. 5 Encryption time comparison

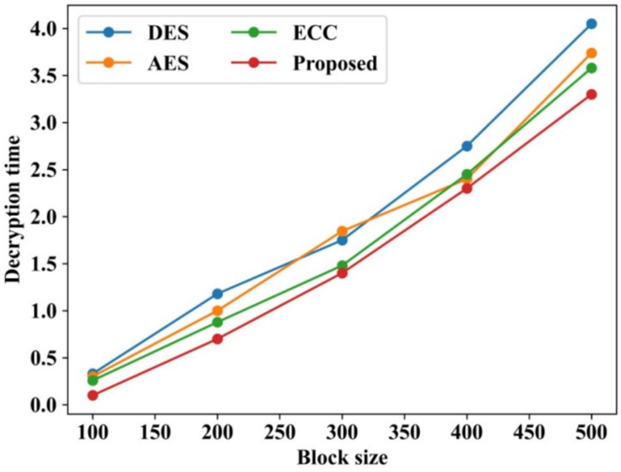


Fig. 6 Decryption time comparison

where d_k is the key vector dimension. For multi-head, the MHA is given as:

$$MHA(Q, K, V) = Con\left(head_1, head_2, \ldots\ldots.., head_H\right)W^0 \tag{25}$$

where H is the overall attention heads and W^0 is the weighting matrices. Every head $head_j$ is computed as:

$$head_j = At\left(QW_j^Q, KW_j^Q, VW_j^Q,\right) \tag{26}$$

The Global Average Pooling (GAP) Layer for minimizing the over-fitting issue and it is placed after the MHA. Finally, the softmax is used for finding the cyber attacks.

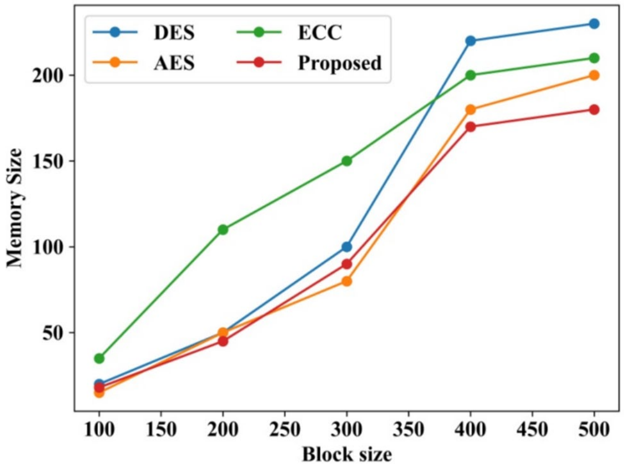


Fig. 7 Memory size comparison

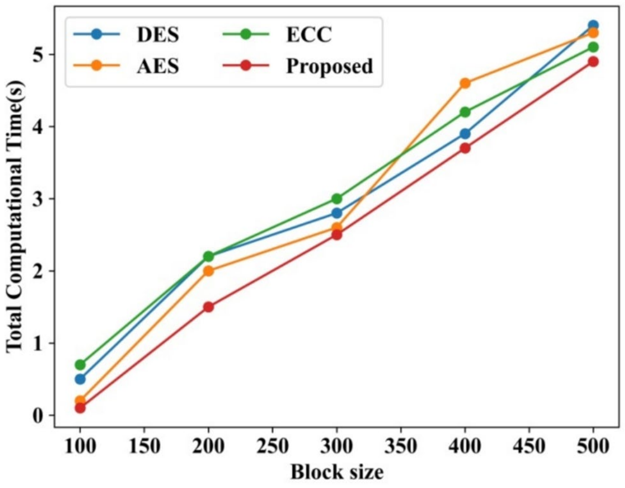


Fig. 8 Total computation time comparison

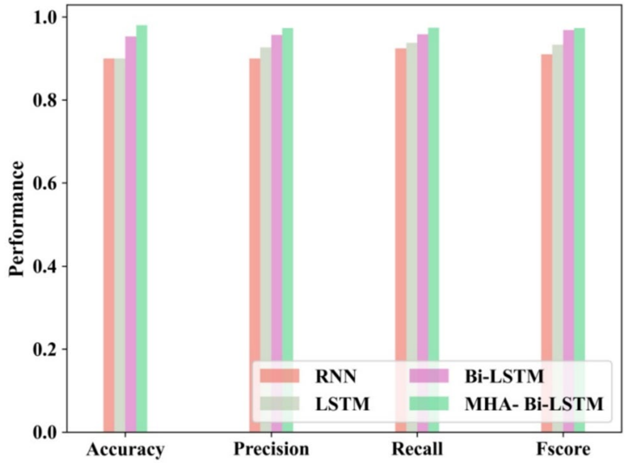


Fig. 9 Comparison of cyberattack measures

4 Results analysis

The following section shows the anlaysis of the suggested and exisiting cyberattack detection model. The experimentation of the work is carried out on Intel core i7-7700 and Python 3.6. The encryption process is demonstrated for methods like Data Encryption Standard (DES), Advanced Encryption Standard (AES), ECC and the proposed ECC-BWK. Then, the cyberattack detection performance is carried out for the methods like RNN, LSTM, Bi-LSTM and MHA- Bi-LSTM.

4.1 Comparitive analysis

Following section shows the comparitive analysis with respect to the data encryption and cyberattack detection.

Figure 5 presents the encryption time comparison of the different approaches like DES, AES, ECC and the proposed ECC-BWK. Encyption time is carried by varying block sizes from 100 to 500. This comparison shows the performance differences and showing how all algorithms handles encryption speed.When the block size is 100, the encryption time attained by the DES, AES, ECC and the proposed ECC-BWK are 0.33 s, 0.3 s, 0.25 s and 0.1 s. Similarly, when the block size is 500, the encryption time attained by the DES, AES, ECC and the proposed ECC-BWK are 4.05 s, 3.74 s, 3.58 s and 3.3 s. Thus, the suggested ECC-BWK attained better performance, enhances key generation efficiency and reduces computational complexity.

Figure 6 presents the Decryption time comparison of the different approaches like DES, AES, ECC and the proposed ECC-BWK. When the block size is 100, the decryption time attained by the DES, AES, ECC and the proposed ECC-BWK are 0.1 s, 0.08 s, 0.09 s and 0.05 s. then, the block size is 200, the decryption time attained by the DES, AES, ECC and the proposed ECC-BWK are 0.6 s, 0.5 s, 0.55 s and 0.45 s. It is observed that for all approaches when the block size is increased, the decryption time is also increasing.

Figure 7 presents the memory size comparison of the different approaches like DES, AES, ECC and the proposed ECC-BWK. It is measured in Kilobyte (KB). This measure reflects the efficiency and resource requirements of all algorithms. This comparison show how much memory all algorithms need during the encryption process, with the proposed ECC-BWK demonstrating optimized memory performance compared to the conventional algorithms. That is the memory size of the proposed ECC-BWK is 18 KB, 45 KB, 90 KB, 170 KB and 180 KB when the block sizes are 100, 200, 300, 400 and 500.

Figure 8 presents the Total computation time comparison of the different approaches like DES, AES, ECC and the proposed ECC-BWK. This comparison evaluates the processing efficiency of all algorithms and highlighting the time required for completing encryption tasks. The proposed ECC-BWK demonstrates improved performance, with reduced computation time compared to traditional methods like DES, AES, and standard ECC. This suggests that ECC-BWK's optimized structure increases encryption speed and creating it more efficient for practical applications. That is the memory size of the proposed ECC-BWK is 0.1 s, 1.5 s, 2.5 s, 3.5 s and 4.9 s when the block sizes are 100, 200, 300, 400 and 500.

Figure 9 shows the comparison of cyberattack measures like accuracy, precision, recall and F-score. The methods like RNN, LSTM, Bi-LSTM and MHA- Bi-LSTM are compared. This comparison illustrates how all models performs in identifying and mitigating cyber threats. An accuracy value achieved by the RNN is 0.9, LSTM is 0.91, Bi-LSTM is 0.95 and MHA- Bi-LSTM is 0.98. The precision value

Fig. 10 ROC curve

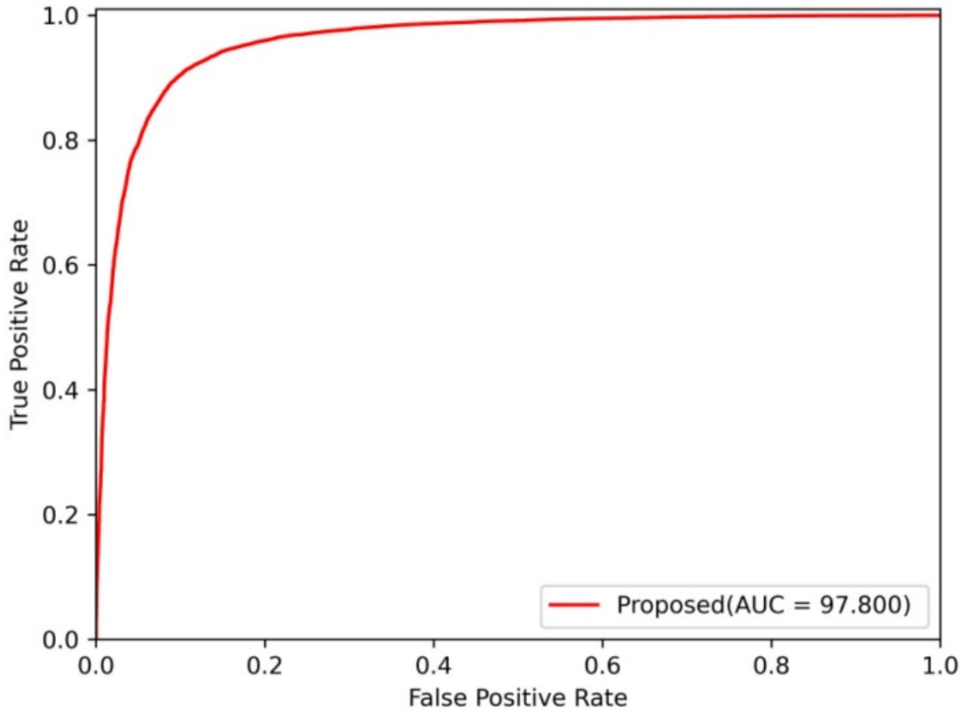
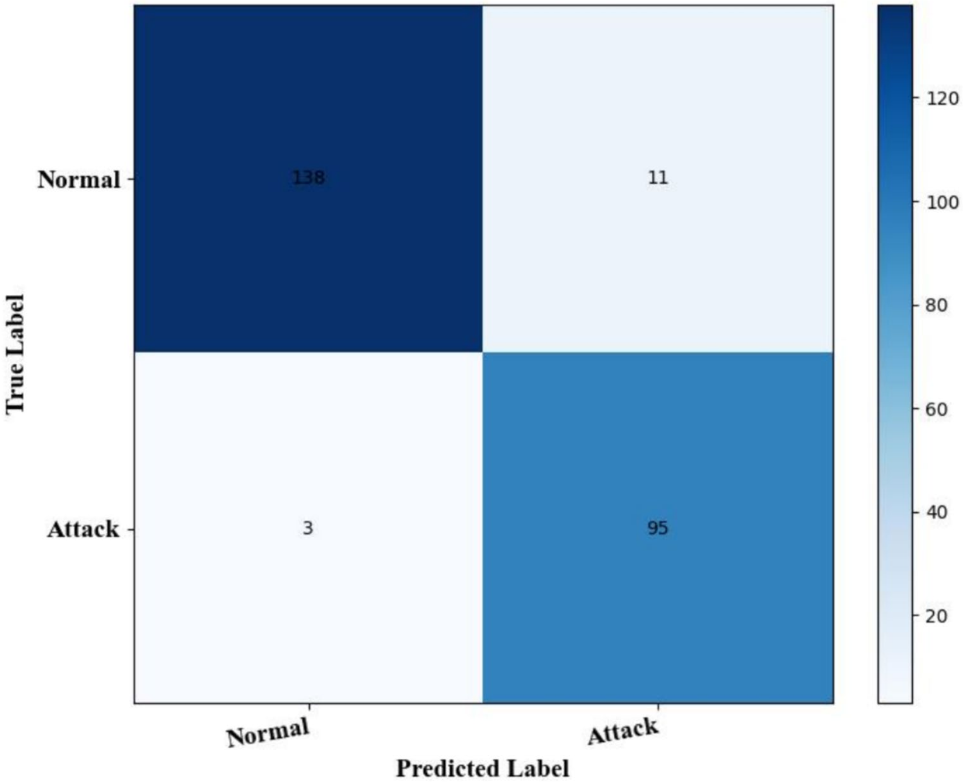


Fig. 11 Confusion matrix



achieved by the RNN is 0.9, LSTM is 0.92, Bi-LSTM is 0.95 and MHA- Bi-LSTM is 0.97. The recall value achieved by the RNN is 0.92, LSTM is 0.93, Bi-LSTM is 0.95 and MHA- Bi-LSTM is 0.97. Finally, the Fscore value achieved by the RNN is 0.93, LSTM is 0.93, Bi-LSTM is 0.96 and MHA- Bi-LSTM is 0.97.

Table 1 Security analysis

Algorithms	KPA	CPA
DES	Vulnerable: Due to its small key size (56 bits), KPA can be evaluated easily, and allow the attackers for analyzing known plaintext-ciphertext pairs	Vulnerable: DES's limited block size and key length make it susceptible to CPA, as patterns can be exploited
AES	Resistant: With large key sizes (128, 192, or 256 bits) and complex encryption, KPA is impractical with modern technology	Resistant: AES's advanced structure and key length make it highly resistant to CPA, especially with secure implementations
ECC	Highly Resistant: The mathematical complexity of ECC makes KPA complex, even with access to plaintext-ciphertext pairs	Highly Resistant: ECC's strong cryptographic structure and use of discrete logarithms provide robust defense against CPA
Proposed ECC-BWK	Very Highly Resistant: Enhanced with the BWK, ECC-BWK offers even greater complexity and efficiency, making KPA practically infeasible	Very Highly Resistant: ECC-BWK optimizes parameter selection, increasing resistance to CPA through reduced computational vulnerability and improved encryption robustness

Figure 10 represents the Region of Characteristics (ROC) curve analysis of the proposed MHA-Bi-LSTM model. The ROC curve presents the model's performance in differentiing between attacks and normal behavior by plotting the True Positive Rate against the False Positive Rate at various threshold settings. The area under the ROC curve (AUC) indicates the model's ability to correctly classify instances. A higher AUC value shows better discrimination ability and the MHA-Bi-LSTM model show its strong performance in accurately detecting cyberattacks and achieved better AUC value 97.8.

Figure 11 represents the confusion matrix of the proposed MHA-Bi-LSTM model. There are 138 samples are categorized as normal and 11 samples are misclassified. There are 95 samples are categorized as attack and 3 samples are misclassified.

4.2 Security analysis

Algorithms like DES, AES, ECC, and the proposed ECC-BWK in terms of their susceptibility to Known-Plaintext Attack (KPA) and Chosen-Plaintext Attack (CPA) are analyzed in Table 1.

KPA: ECC-BWK shows exceptional resistance to KPA because of the essential complexity of ECC combined with the BWK optimization. The ECC is based on the complexity of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). This creates it extremely challenging for attackers for deriving the private key even with known plaintext-ciphertext pairs. The BWK optimization enhances this by improving key generation and parameter selection, reducing potential vulnerabilities.

CPA: ECC-BWK ensures strong defense against CPA. The combination of BWK optimizes encryption processes and provides that key parameters are dynamically selected for resisting attempts to predict ciphertext outcomes. This advanced model prevents attackers from gaining essential information by submitting chosen plaintext and maintains the confidentiality and integrity of the system.

5 Conclusion

The proposed model has the stages like encryption, data storage, decryption, and cyberattack detection. In this suggested model, the ECC with BWK model integrated with BC offers a robust and efficient solution. Then, the DL model MHA-Bi-LSTM provided better cybersecurity in IoT environments. By considering the strengths of ECC, which ensured high security with smaller key sizes, and the BWK optimization, improves key generation and cryptographic processes, the suggested model addressed key cybersecurity limitations like data integrity, authentication, and secure communication in

IoT networks. The integration with BC offered decentralized, and transparent, making the system resistant to several cyber threats. The model has demonstrated superior resistance to KPA and CPA through extensive performance evaluations compared to traditional cryptographic methods. Then, with respect to the cyberattack detection accuracy and precision values achieved were 0.98 and 0.97 on the CICIoT2023 dataset. The combination of ECC and BWK optimization offers high encryption and decryption times by varying block size from 100 to 500 and developing it suitable for IoT applications with resource constraints. The analysis demonstrated that the suggested model remarkably improves threat detection accuracy and also offers a scalable solution to secure IoT networks. In the future, since quantum computing is emerging, combining post-quantum cryptographic techniques into the ECC and BC framework may provide future proof security and ensure resistance to potential quantum based attacks. The MHA-BiLSTM model will be enhanced by integrating external threat intelligence data sources for improving its ability in predicting and responding to emerging cyber threats in real-time.

Data availability Data will be made available upon reasonable request.

Declarations

Conflict of 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. Shafay M, Ahmad RW, Salah K, Yaqoob I, Jayaraman R, Omar M (2023) Blockchain for deep learning: review and open challenges. Clust Comput 26(1):197–221. https://doi.org/10.1007/s10586-022-03582-7
2. Ferrag MA, Maglaras L (2020) DeepCoin: a novel deep learning and blockchain-based energy exchange framework for smart grids. IEEE Trans Eng Manage 67(4):1285–1297. https://doi.org/10.1109/tem.2019.2922936
3. Wylde V, Rawindaran N, Lawrence J, Balasubramanian R, Prakash E, Jayal A, Khan I, Hewage C, Platts J (2022) Cybersecurity, data privacy and blockchain: a review. SN Comput Sci 3(2):127. https://doi.org/10.1007/s42979-022-01020-4
4. Goel A, Agarwal A, Vatsa M, Singh R, Ratha N DeepRing: protecting deep neural network with blockchain. In: 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 16–17 June 2019 2019. pp 2821–2828. https://doi.org/10.1109/cvprw.2019.00341
5. Mishra S, Chaurasiya VK (2024) Hybrid deep learning algorithm for smart cities security enhancement through blockchain and internet of things. Multimedia Tools Appl 83(8):22609–22637. https://doi.org/10.1007/s11042-023-16406-6
6. Ogundokun RO, Arowolo MO, Misra S, Awotunde JB (2022) Machine learning, IoT, and blockchain integration for improving process management application security. In: Misra S, Kumar Tyagi A (eds) Blockchain Applications in the Smart Era. Springer International Publishing, Cham, pp 237–252. https://doi.org/10.1007/978-3-030-89546-4_12
7. Malik S, Malik PK, Naim A (2024) Opportunities and challenges in new generation cyber security applications using artificial intelligence, machine learning and block chain. In: Kaushik K, Sharma I (eds) Next-Generation Cybersecurity: AI, ML, and Blockchain. Springer Nature Singapore, Singapore, pp 23–37. https://doi.org/10.1007/978-981-97-1249-6_2
8. Moyeenudin HM, Bindu G, Anandan R (2024) Blockchain networks for cybersecurity using machine-learning algorithms. In: Goundar S, Anandan R (eds) Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations. Springer International Publishing, Cham, pp 233–242. https://doi.org/10.1007/978-3-031-35751-0_16
9. Pan X, Zhong B, Sheng D, Yuan X, Wang Y (2022) Blockchain and deep learning technologies for construction equipment security information management. Autom Constr 136:104186. https://doi.org/10.1016/j.autcon.2022.104186
10. Chen D, Wawrzynski P, Lv Z (2021) Cyber security in smart cities: a review of deep learning-based applications and case studies. Sustain Cities Soc 66:102655. https://doi.org/10.1016/j.scs.2020.102655
11. Ahmad J, Zia MU, Naqvi IH, Chattha JN, Butt FA, Huang T, Xiang W (2024) Machine learning and blockchain technologies for cybersecurity in connected vehicles. WIREs Data Min Knowl Discovery 14(1):e1515. https://doi.org/10.1002/widm.1515
12. Nguyen GN, Viet NHL, Elhoseny M, Shankar K, Gupta BB, El-Latif AAA (2021) Secure blockchain enabled cyber–physical systems in healthcare using deep belief network with ResNet model. Journal of Parallel and Distributed Computing 153:150–160. https://doi.org/10.1016/j.jpdc.2021.03.011
13. Rathore S, Park JH (2021) A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems. IEEE Trans Industr Inf 17(8):5522–5532. https://doi.org/10.1109/tii.2020.3040968
14. Unal D, Hammoudeh M, Khan MA, Abuarqoub A, Epiphaniou G, Hamila R (2021) Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. Comput Secur 109:102393. https://doi.org/10.1016/j.cose.2021.102393
15. Kumar P, Kumar R, Aljuhani A, Javeed D, Jolfaei A, Islam AKMN (2023) Digital twin-driven SDN for smart grid: a deep learning integrated blockchain for cybersecurity. Sol Energy 263:111921. https://doi.org/10.1016/j.solener.2023.111921
16. Veeramakali T, Siva R, Sivakumar B, Senthil Mahesh PC, Krishnaraj N (2021) An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. J Supercomput 77(9):9576–9596. https://doi.org/10.1007/s11227-021-03637-3
17. Neto ECP, Dadkhah S, Ferreira R, Zohourian A, Lu R, Ghorbani AA (2023) CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. Sensors 23(13):5941

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.