Security Assessment Framework for IOT via Glove Optimized CNN-BiLSTM

Original Scientific Paper

Arun V
Department of Computing Technologies, School of Computing,
SRM Institute of Science and Technology,
Kattankulathur, Chengalpattu 603203, India
arun.AR543@outlook.com

Ramesh S
Department of Computer Science Engineering,
Krishnasamy College of Engineering Technology,
Anand Nagar, Kumarapuram, Cuddalore, India
remesh765@gmail.com

Carmel Sobia M
Department of Electrical and Electronics Engineering,
PSR Engineering College, Sivakasi, Tamil Nadu
626140, India
sobia654@gmail.com

Geetha A
Department of Electrical and Electronics Engineering,
PSR Engineering College, Sivakasi, Tamil Nadu
626140, India
geetha32GA@gmail.com

Abstract *– The Internet of Things (IoT) is a vast network of real, tangible objects or "things" that can communicate and share data with other systems and gadgets over the Internet. A vital component of assuring the secure and dependable operation of IoT systems and devices is IoT security. Attackers may use IoT devices to get unauthorized access, change functionality, or compromise the data that the device collects and transmits. The risks of IoT security breaches grow as more devices connect and exchange sensitive data. To check the vulnerability in Iot devices, a novel Blockchain enabled Iot based Security Assessment for intrusion (Block-ISAI) technique has been proposed. Bag of Words (BoW) technique is used for feature extraction of API documents which helps to make the document simpler. Blockchain technology is utilized for secure data storage and IoT device registration. In order to detect intrusion, a deep learning architecture is designed using the verified data The attack is either detected or not detected when the vulnerability is found using the GloVe-CNN-BiLSTM Model. If the vulnerability is detected then alerts will be given. Utilizing evaluation measures like accuracy, time efficiency, precision, F1 score, detection rate, recall, false alarm rate, usability and reliability the efficacy of the suggested ISAI technique has been assessed. By the comparison analysis, the proposed ISAI technique's detection rate is 18.22%, 19.43%, and 3.13% higher than the existing HIDS, NIDS, and ML-DDoS techniques respectively. The accuracy of the proposed system is increased by 0.69%, 6.04%, and 36.15% as compared to the HIDS, NIDS, and ML-DDoS method using UNSW-NB 15 dataset and increases by 2.37%, 18.32%, and 5.95% using KDDCUP 19 dataset respectively.*

Keywords: *Internet of things, Security assessment, Vulnerabilities, Bag of words, deep learning*

Received: September 8, 2023; Received in revised form: January 23, 2024; Accepted: January 23, 2024

1. INTRODUCTION

Internet of Things (IoT) is to connect a collection of connected objects so that they may exchange data and communicate with one another online [1]. Its applications extend across numerous industries, enabling companies, boosting productivity, and raising people's quality of life all across the world [2]. IoT's fundamental idea is that by enabling communication between linked things and people, a massive network of interconnected devices can be built [3-5]. Smart homes, healthcare, transportation, agriculture, manufacturing, and many other sectors and businesses have the potential to undergo major transformations as a result of IoT technology [6].

Device security, which focuses on protecting specific devices from unwanted access, tampering, or exploitation, is a vital component of IoT security [7]. Making sure that only permitted parties can access and control IoT devices, entails designing secure hardware and firmware designs, enabling encryption methods, and utilizing authentication techniques [8,9]. IoT device security is used for the security procedures implemented to protect IoT devices and the data they gather, transport, and store [10]. IoT devices are real-life objects that have sensors, software, and connection built into them so they can communicate with other IoT devices and systems via the Internet [11, 12]. A block, which is a sort of digital information, and a chain, which is an open database, make up the first blockchain. As soon as in-

formation is embedded into the immutable sequence of blocks, it becomes impossible to change, providing protection against data poisoning attacks [12]. Decentralized architecture enables smart contracts to improve trust between the parties involved in data transfer. These smart contracts carry out and enforce the conditions of the contract on their own. Moreover, consensus processes provide an extra degree of security by securing the integrity of the distributed data stored in the blockchain [13].

IoT devices regularly capture and communicate sensitive data, such as private information, health data, or financial details. If vulnerabilities are present and not discovered, hackers may use them to intercept data or obtain unauthorized access to the device. IoT device adoption has increased worries regarding security, privacy, and dependability [14]. IoT devices could include security flaws that would be easy for bad actors to use if vulnerability detection wasn't present [15]. The need to address potential vulnerabilities and defend against malicious attacks is becoming more and more important as the number of IoT devices increases. In this paper, a novel Blockchain enabled IoT based Security Assessment for intrusion (Block-ISAI) technique has been proposed to detect the vulnerability attack in IoT devices. The following is a list of the paper's main contributions.

- Initially, API documents are collected from the IoT vendors and then the API document undergoes into feature extraction process.
- In the feature extraction process, the document is analyzed and the Bag of Words (BoW) technique is used for feature extraction and then the output is given to the input message creation module from the feature extraction module.
- A new input message is created and the text message is given to the IoT devices, it generates the response and it is verified by the verifier.
- Blockchain technology is utilized for secure data storage and IoT device registration. In order to detect intrusion, a deep learning architecture is designed using the verified data.
- The vulnerability is detected by using the GloVe-CNN-BiLSTM Model and the output is generated as attack detected and attack not detected.

The remainder of this study is explained in the manner that follows: Section II analyses the study based on the literature. Section III provides a detailed description of the proposed system. Section IV represents the result and discussion, and Section V represents the conclusion.

2. LITERATURE REVIEW

In 2019, Khraisat et al. [16] suggested a unique ensemble Hybrid Intrusion Detection System (HIDS) to safeguard Internet of Things devices. The findings indicate that, in comparison to SIDS and AIDS methods, the suggested hybrid IDS yields a higher detection rate and a smaller percentage of false positives. In 2021, Roy and Srirama [17] suggested a decentralized security system for the Internet of Things (IoT) mobile edge and fog computing. The trial results shows that it outperforms all other methods in its sector and can be used effectively and efficiently as a security feature.

In 2021, Kumar et al., [18] presented a fog-cloud architecture-driven framework for ensemble learning that is used to detect cyberattacks on Internet of medical devices. The experimental results show that the it can achieve 99.98% detection rates, an accuracy of 96.35, and limit false alarm rates up to 5.59%. In 2021,

In Qaddoura et al. [19] recommended a strong intrusion detection system that makes use of a thorough multi-layer categorization method. The proposed technique outperforms the alternatives in terms of the G-mean, which is 78% instead of KNN's 75%.

In 2021, Awotunde et al. [20] proposed several Network Intrusion Detection Systems (NIDSs) to defend and combat IIoT systems in terms of FPR, detection rate, and accuracy, the recommended technique outperforms other pertinent methods by 99.0%, 99.0%, and 1.0%, respectively. In 2022, Hamza et al. [21] suggested the HSAS-MD analyzer, a new hybrid (static and dynamic) SAS that highlights IoT programs from a thorough analytical perspective. The results of the test indicate that HSAS-MD provides 93%, 91%, 94%, and 95% F-measure, recall, precision, and accuracy, respectively.

In 2022, Hayat et al. [22] suggested a multilayer DDoS mitigation technique (ML-DDoS) that uses a blockchain-based infrastructure to protect devices. The findings show that, proposed framework offers up to 35% throughput improvement, up to 40% latency improvement, and up to 25% better CPU utilization.

The comparison table of existing methods are given in the Table 1.

Table 1. Comparison with existing Techniques

Authors	Methods	Evaluation Criterion	Results
Khraisat et al. [16]	HIDS	True positive rate, F-measure, false positive rate, and accuracy	The accuracy of malware detection is 94%.
Roy and Srirama [17]	Security system for the IoT mobile edge and fog computing with block chain	Mathew correlation coefficient (MCC), Positive Predictive Value (PPV), Identification Rate (IR), Accuracy, F-Score, Identification Time (IT)	It has the accuracy of 95.2%
Kumar et al. [18]	Ensemble learning and fog-cloud architecture-driven cyber-attack detection framework.	Accuracy, precision, detection rate, F1 score and false alarm rate	The experimental results show a 99.98% detection rate, a 96.35% accuracy rate.

Qaddoura et al. [19]	A deep multi-layer classification approach	Accuracy, Recall, and G-mean measures	G-mean's value of 78% is in contrast to KNN's 75%
Awotunde, et al. [20]	NIDS	F1-score, recall, specificity, accuracy, and precision	Accuracy, detection rate, and FPR by 99.0%, 99.0%, and 1.0%, respectively
Hamza et al. [21]	HSAS-MD analyzer	Assessed using the widely accepted metrics of recall, accuracy, precision, and F1 score	For accuracy, precision, recall, and F-measure, it offers 95%, 94%, 91%, and 93%, respectively
Hayat et al. [22]	ML-DDoS	Precision of detection, efficacy of mitigation, scalability, and resilience against hostile assaults	It improves throughput by up to 35%, latency by up to 40%, and CPU utilization by up to 25%

3. BLOCKCHAIN ENABLED IOT BASED SECURITY ASSESSMENT FOR INTRUSION (BLOCK-ISAI) TECHNIQUE

In this paper, a novel Blockchain enabled Iot based Security Assessment for intrusion (Block-ISAI) technique has been proposed to detect vulnerabilities in IoT devices. Initially, API documents are collected from the IoT vendors and then the API document undergoes into feature extraction process. These API docs provide details on the acceptable inputs for calling the API-based functionality of IoT devices. The Bag of Words (BoW) algorithm is used for feature extraction of API documents provided by the IoT vendors a new input message is created and the text message is given to the IoT devices, it generates the response and it is verified by the verifier. Blockchain technology is utilized for secure data storage and IoT device registration. In order to detect intrusion, a deep learning architecture is designed using the verified data. GloVe-CNN-BiLSTM Model is used to detect vulnerability in IoT devices. The proposed Block-ISAI method's whole framework is shown in Fig 1.

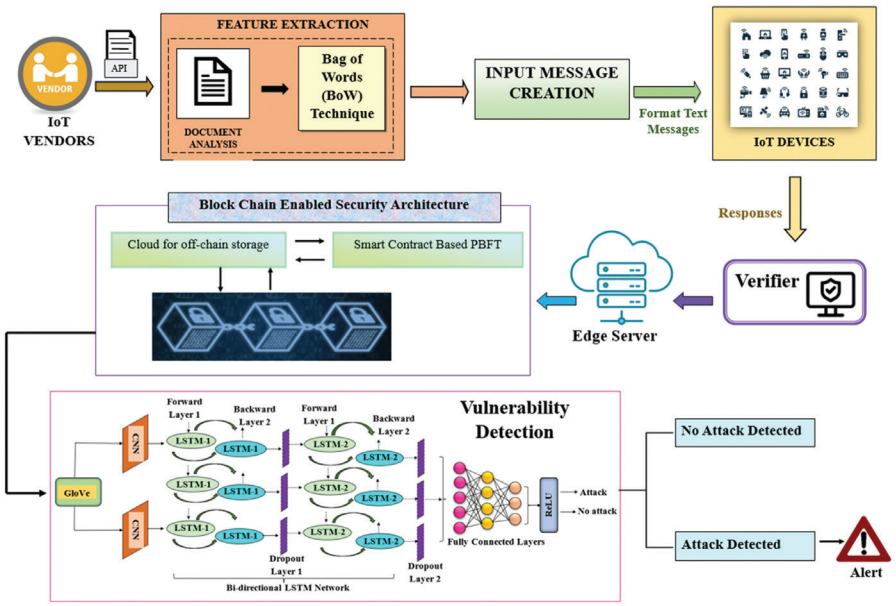

Fig. 1. Blockchain enabled IoT-based Security Assessment for Intrusion (Block-ISAI) Framework

3.1. API DOCUMENTS FOR IOT DEVICES

To assist developers in using their device APIs, the majority of IoT vendors publish an API document. The API document is semi-structured, published in HTML pages, and is available to the public on the Internet. The specifics of the API requirements are usually the first section of an API document. API specifications are information obligatory to construct an appeal note to use a certain device API.

3.2. FEATURE EXTRACTION

In the feature extraction process, the Bag of Words (BoW) technique is used for extracting features and analyzing the document is a key stage, especially when working with textual materials.

3.2.1 Bag of Words (BoW) technique

The Bag of Words is a simple and commonly used feature extraction technique. Text representation is the first step for a machine to comprehend the text. The formula for the bag of words representation of a document is given in (1).

$$bow(d_o)=[count(w_{o_1}, d_o), count(w_{o_2}, d_o)..., count(w_{o_n}, d_o)] \quad (1)$$

Where n represents vocabulary size and the document as d_o, $bow(d_o)$ represents the bag of words representation. Text tokenization is the process of segmenting text into words by utilizing white space and punctuation as delimiters. Using the BoW technique, every document is represented by a numerical vector,

resulting in a fixed feature set. Word frequency in the document is indicated by values in the vector. Formula (2) expresses the BoW design.

$$z=[z_1, z_2, z_3,.....z_n] \quad (2)$$

Where, $z_j = n_j$ if the j-th word appears in the text and $z_j = 0$ if the j-th word does not appear in the text. Two types of features—permission and API function calls—are extracted from the API specification using the BOW approach. The permissions may be collected from the manifest files, and the API function calls are taken from the Java source files. Then, they will include the two collections into the feature set, which serves as an input for the deep learning network's training and testing purposes. Two classes can be distinguished from the classification result based on the DL model. Table 2 provides some instances for the List of Permission Feature Groups from the API document.

Table 2. Permission Feature Groups from API document

Permission Group	Permissions
CALENDAR	android. permission. READ_CALENDAR android. permission. WRITE_CALENDAR
STORAGE	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE
SENSORS	android.permission.BODY_SENSORS android.permission.USE_FINGERPRINT

3. 3. INPUT MESSAGE CREATION

The feature extraction module generates numerical vectors for the input message creation, aligning with target IoT device APIs. User-configured values serve as templates, with default parameters in input vectors. In the advanced block, unnecessary parameters are randomly discarded, and missing ones are created. The module efficiently updates a parameter subset, ensuring a formatted message is sent to IoT devices. Responses are directed to a blockchain-enabled security architecture. Fig 2 shows the proposed ISAI technique's flow chart.

3.4. BLOCK CHAIN ENABLED SECURITY ARCHITECTURE

Six separate processes comprise the first degree of security: 1) Starting; 2) Registration and Authentication; 3) Encoding and Decoding; 4) Block Generation and Verification; 5) Data Creation and Updation of block; and 6) Consensus. Below is a full explanation of how each phase operates.

3.4.1. Starting Phase

In order to register the IoT device (ID), the trusted verifier (V_r) assesses this phase and bootstraps the framework parameters. Stage 1: The verifier (V_r) selects the largest prime value (BP_m) suitable for a non-singular elliptical arc. Random generator g is chosen for $g1$, and bilinear mapping b, is established from $g1 \times g1 \rightarrow g2$. Stage 2: The $Pr_{Vr}k$ (private key) is selected at random by the verifier.

Detailed explanation is as follow

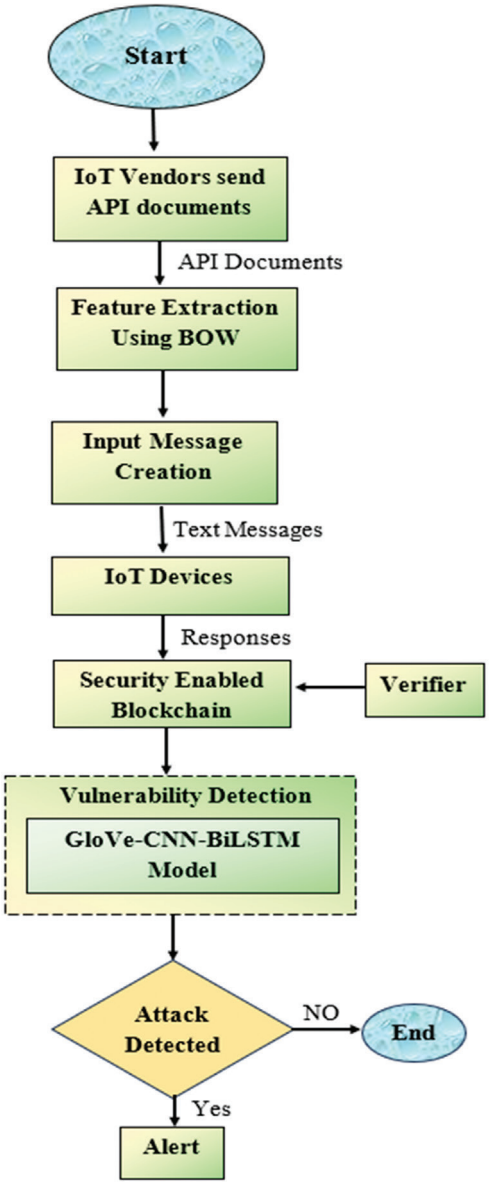

Fig. 2. Flowchart of the proposed Block-ISAI method

Next, $Pb_{Vr}k = Pr_{Vr}k$ is used to generate the public key, or $Pb_{Vr}k$ where $K.g$ stands for multiplication points on an elliptic curve. Stage 3: Vr then selects the one-way cryptographic hash function $Hh(.)$.

3.4.2. Registration and Authentication Phase

IoT device ID requests verifier Vr to join the blockchain (BC) network during the registration step. The IoT device's mac address (M_{ID}) and device identification (i_{ID}) are the two main components that ID uses to construct the provisional key PL_K. Timestamp (TS_j) is saved for ID registration verification when the PL_K is successfully produced. Both PL_K, along with matching i_{ID} and M_{ID}, are sent to the verifier.

3.4.3. IoT-generated data encryption and decryption Phase

Following the successful registration of the IoT device (ID) with the verifying authority, V_r is a public key Pb_{ID} and Pr_{ID} private key is produced. Next, the secret keySK_{ID} is computed over the infinite field ZBP_m and random picked point BP_m over the elliptic curve. Equations (3) and (4) illustrated the two distinct ciphertexts from which the encrypted data are separated.

$$C_a = (BP_m 1 \times BP_m) + SK_{ID} \quad (3)$$

$$C_b = M + (BP_m 1 + Pb_{ID}) + SK_{ID} \quad (4)$$

$$M = ((C_a - Pb_{ID}) \times C_a - SK_{ID} \quad (5)$$

The message created by an IoT device is represented by M, while C_a and C_b indicate the ciphertext. Equation 5 is finally used to decrypt the message.

3.4.4. Block Generation and Verification phase

The process of creating and validating blocks begins after a successful ID registration. Stage 1: The first step consists of key pairs for IoT devices (ID), such as Pb_{ID} and, where Pb_{ID} is a public key and Pr_{ID} is a private key. Stage 2: Ed generates Ed_{sg} and sends it to ID for verification. ID validates the signature, and submits a request for Ed_{sg} to join the BC network. Stage 3: A new block i_{ID}^{block} is created and sent for blockchain.

3.4.5. Data Creation and Updation of Block

This stage explains the process of creating data and updating the corresponding block. Stage 1: Initially, a new transaction (i_{ID}^{NTC}) is established along with Sig_{ID}, Pb_{ID}, and i_{ID} of ID. Stage 2: Furthermore, records are verified Pb_{ID} for the corresponding i_{ID}, in addition to i_{ID}^{TC} and Sig_{ID}. Stage 3: Further, i_{ID}^{block} is successfully appended to the BC network and updated.

3.4.6.Consensus Phase

The i_{ID} is generated, transmitted to IoT devices, and integrated into the BC following ZP verification. The PBFT consensus technique is employed for transaction authentication and addition to the blockchain network (i_{ID}^{TC} by i_{ID}). The SHA-512 algorithm computes the transaction hash and the block is added to the BC.

3.5. GLOVE-CNN-BILSTM MODEL

GloVe-CNN-BiLSTM Model is the combination of Global Vectors for Word Representation (GloVe) with Convolution Neural Networks-Bidirectional Long Short-Term Memory (CNN-BiLSTM) algorithm to detect the vulnerability in the IoT devices.

3.5.1. GloVe Model

A GloVe model is a useful tool for using data from the global corpus and adjusting the learning model based on the context window. The following equation (6) can be used to define the GloVe model:

$$K = \sum_{j,i}^{M} f(Y_{ji}) \left[W_j^T W_i + a_j + a_i - \ln(Y_{ji})\right]^2 \quad (6)$$

where Y is the cooccurrence matrix, Y_{ji} represents how many times the terms j and i appear together in a single window, W_j and W_i stand for the word vectors of j and i. M is the dimension of the cooccurrence matrix $M \times M$, a_j and a_i are the deviation terms, and f is the weight function. The following is the formula for $f(y)$:

$$f(y) = \begin{cases} (y/y_{max})^{\alpha}, & y < y_{max} \\ 1, & y \geq y_{max} \end{cases} \quad (7)$$

3.5.2. CNN-BiLSTM Model

The GloVe model output is fed into the CNN-BiLSTM Model for vulnerability detection. the CNN structure comprises input, pool, and convolution layers, followed by a classifier. For a comment message M={m(1),m(2),…..,m(n)}, each word $w_o(j)$ is transformed into the corresponding word vector $V_e(w_o(j))$ by GloVe, generating a sentence matrix SM_{ji} (8) from the word-by-word statement $w_o(j)$.

$$SM_{ji} = \{V_e(w_o(1)), V_e(w_o(2)), \ldots \ldots V_e(w_o(j))\} \; 1 \leq j \leq n \quad (8)$$

SM_{ji} is the convolution layer's input in the CNN model, and the convolution layer convolves SM_{ji} with a size filter $s \times t$ to derive the regional semantic traits of SM_{ji}. The calculation formula is given in (9)

$$b_{ji} = f(F_l \times V_e(w)(j: j + s - 1) + a) \quad (9)$$

Where, F_l represent the filter of $s \times t$, f indicates the ReLU nonlinear conversion Finally, all pooled attributes are integrated at the entire connection layer to produce the output vector.

$$i_s = \sigma(V^i y_s + X^i h_{s-1}) \quad (10)$$

Let, i_s be the input gate function of the BiLSTM network at time s and V^i, X^i are the weight matrices.

$$f_s = \sigma(V^f y_s + X^f h_{s-1}) \quad (11)$$

In (11), f_s denotes the forget gate function at time step s, σ is the activation function, V^f, X^f indicates the weight matrices of the forget gate function. h_s is the hidden state at time step s.

$$o_s = \sigma(V^o y_s + X^o h_{s-1}) \quad (12)$$

From equation (12), o_s is the output gate function, y_s is the input at the time step s. V^o, X^o are the weight matrices of the output gate function.

$$c'_s = tanh(V^c y_s + X^c h_{s-1}) \quad (13)$$

$$c_s = i_s \times c'_s \times f_s \times c'_{s-1} \quad (14)$$

In equations (13), (14), c_s and c_s' are the cell state during time step s, h_{s-1} is the concealed state and tanh is the hyperbolic tangent activation function.

$$h_s = o_s \times \tanh(c_s) \quad (15)$$

h_s represents the LSTM cell's final hidden state at the most recent time step (s), while o_s denotes the output gate activation at the last time step (s).

The BiLSTM model integrates past and future knowledge using feature data from time *t*. The CNN pooling layer's output, feeds into opposing LSTM networks. Both forward and backward LSTMs capture input sequence information. Vector splicing produces the final hidden layer representation. The GloVe-CNN-BiLSTM Model issues alerts upon detecting attacks.

4. RESULT AND DISCUSSION

The experimental results of the Block-ISAI method are analyzed, and performance is discussed using various evaluation metrics. KDDCUP 19 and UNSW 15 datasets are employed for assessment. Effectiveness is compared with HIDS [16], NIDS [20], and ML-DDoS [22] across F1-Score, accuracy, detection rate, precision, false alarm rate, usability, and reliability.

4.1. DESCRIPTION OF DATASETS

The KDDCUP 19 dataset, a subset of the 1998 DARPA IDS evaluation program, features 28 dimensions out of 41, totalling 31,279 instances. Additionally, the ISCX subset contributes 33,746 instances. The UNSW-NB15 dataset, with 42 features (39 numeric, 3 categorical), is split into UNSW-NB15-TRAIN for training and UNSW-NB15-TEST for testing, serving as a crucial evaluation resource [23-25].

4.2. COMPARATIVE ANALYSIS

This section includes simulations to evaluate the effectiveness of the proposed technique.

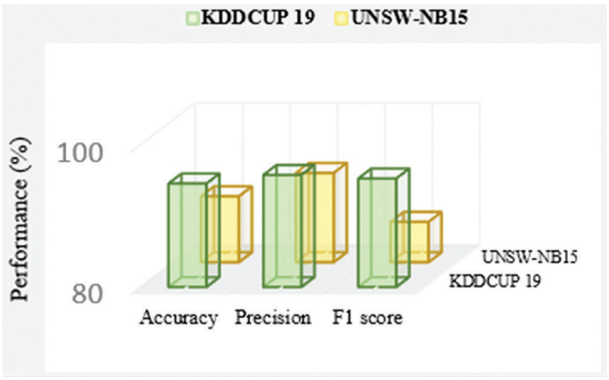

Fig. 3. Performance Comparison

Fig 3 evaluates model performance on KDDCUP 19 and UNSW-NB 15 datasets. For KDDCUP 19, the model achieves outstanding accuracy, precision, and F1 score of 94.6%, 95.8%, and 95.3%. On UNSW-NB 15, it demonstrates strong performance with scores of 89.3%, 92.6%, and 85.7% for accuracy, precision, and F1 score.

Fig 4 compares the accuracy of the proposed Block-ISAI strategy with other approaches (HIDS, NIDS, ML-DDoS) using KDDCUP 19 and UNSW-NB 15 datasets. Our method exhibits significant accuracy improvements of 0.69%, 6.04%, and 36.15%, showcasing superior vulnerability detection compared to existing techniques.

In Fig. 5, the performance comparison of the proposed ISAI technique and existing methods (HIDS, NIDS, ML-DDoS) is depicted, focusing on detection rates using datasets. The Block-ISAI technique exhibits a superior detection rate, surpassing HIDS, NIDS, and ML-DDoS by 18.22%, 19.43%, and 3.13% respectively

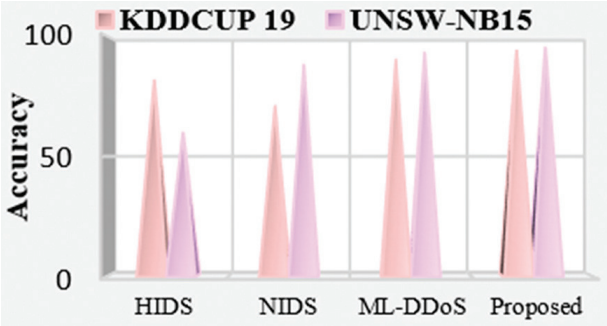

Fig. 4. Performance comparison in terms of accuracy

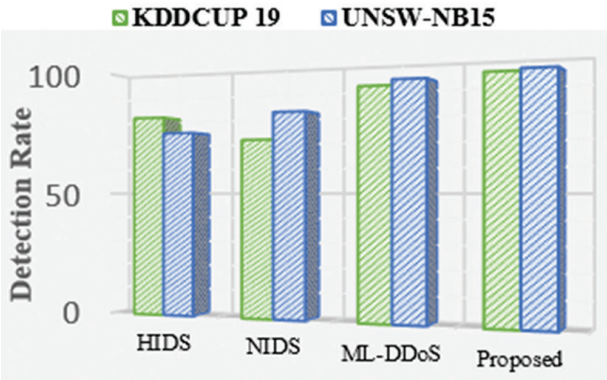

Fig. 5. Comparison in terms of detection rate

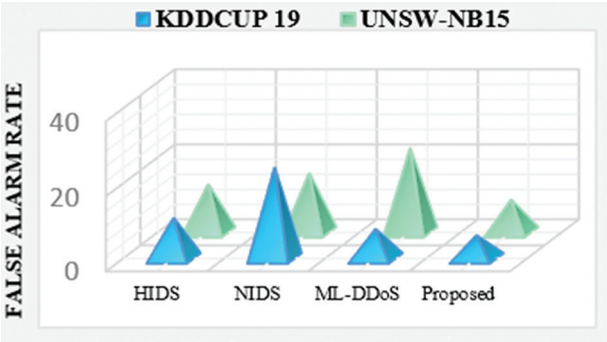

Fig. 6. Comparison in terms of False alarm rate

Fig. 6 compares false alarm rates of our ISAI technique with HIDS, NIDS, ML-DDoS using datasets. Block-ISAI exhibits a lower false alarm rate, demonstrating greater accuracy in threat identification compared to HIDS, NIDS, and ML-DDoS.

Fig. 7 displays results of a blockchain-driven security architecture examination. Block generation and access timings (Figs. 7a and 7b) show stability at 350 TC with up to 40 nodes. However, with 80 nodes, block creation and access take longer than with 60, highlighting scalability challenges in blockchain systems with increased nodes.

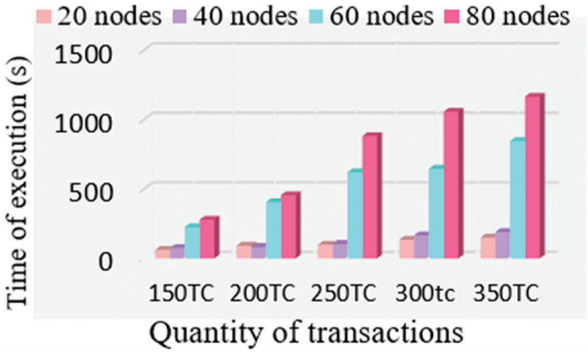

Fig. 7. (a) Block access time across various transaction sizes (TCs)

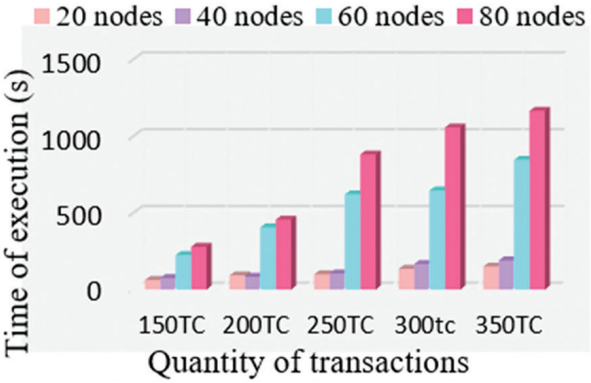

Fig. 7 (b). Block creation time across various transaction sizes (TCs)

Fig. 8 compares our blockchain-enabled IoT security assessment method with traditional approaches, highlighting superior usability and reliability. Enhanced usability comes from a user-friendly interface and robust data integrity procedures, while the decentralized blockchain foundation ensures heightened security for IoT ecosystems.

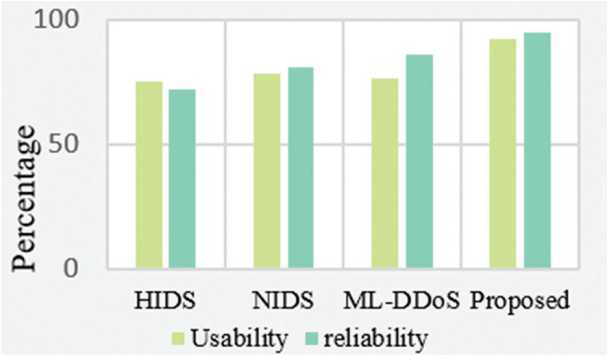

Fig. 8. Comparison in terms of usability and reliability

5. CONCLUSION

In this paper, a novel blockchain enabled IoT based Security Assessment Intrusion (Block-ISAI) technique has been proposed to detect the vulnerability in IoT devices. By extracting the most pertinent and important information, feature extraction helps to make the document simpler. Blockchain technology is utilized for secure data storage and IoT device registration. The vulnerability is detected by using GloVe-CNN-BiLSTM Model and the output is generated as attack detected and attack not detected. The effectiveness of the proposed Block-ISAI technique has been determined using evaluation metrics such as false alarm rate, accuracy, recall, precision, detection rate, F1 score, usability and reliability. According to the comparative analysis, the accuracy of the proposed system is increased by 0.69%, 6.04%, and 36.15% as compared to the HIDS, NIDS, and ML-DDoS method using UNSW-NB 15 dataset and increases by 2.37%, 18.32%, and 5.95% using KDDCUP 19 dataset. Future work will focus on developing user-friendly interfaces for simple configuration, management, and monitoring of security assessments.

6. REFERENCES

[1] A. M. Rahmani, S. Bayramov, B. K. Kalejahi, "Internet of Things Applications: Opportunities and Threats", Wireless Personal Communications, Vol. 122, No.1, 2022, pp. 451-476.

[2] R. Sissodia, M. S. Rauthan, V. Barthwal, "Challenges in Various Applications Using IoT", Handbook of Research on Machine Learning-Enabled IoT for Smart Applications Across Industries, IGI Global, 2023, pp. 1-17.

[3] B. Chander, S. Pal, D. De, R. Buyya, "Artificial Intelligence-based Internet of Things for Industry 5.0", Artificial intelligence-based Internet of things systems, Springer, 2022, pp. 3-45.

[4] K. Elgazzar, H. Khalil, T. Alghamdi, A. Badr, G. Abdelkader, A. Elewah, R. Buyya, "Revisiting the internet of things: New trends, opportunities and grand challenges", Frontiers in the Internet of Things, Vol. 1, 2022, p. 1073780.

[5] F. Firouzi, B. Farahani, M. Weinberger, G. DePace, F. S. Aliee, "IoT fundamentals: Definitions, architectures, challenges, and promises", Intelligent Internet of Things: From Device to Fog and Cloud, Springer, 2020, pp. 3-50.

[6] I. Ahmed, Y. Zhang, G. Jeon, W. Lin, M. R. Khosravi, L. Qi, "A blockchain-and artificial intelligence-enabled smart IoT framework for sustainable city", International Journal of Intelligent Systems, Vol. 37, No. 9, 2022, pp. 6493-6507.

[7] E. R. K. Sen, E. A. Dash, "Unveiling the Shadows: Exploring the Security Challenges of the Internet of Things (IoT)", International Journal of Scientific

Research and Management, Vol. 7, No. 7, 2023 pp. 1-12.

[8] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, H. A. Alkhzaimi, "Cryptography Algorithms for Enhancing IoT Security", Internet of Things, Vol. 22, 2023, p. 100759.

[9] K. Balasamy, N. Krishnaraj, J. Ramprasath, P. Ramprakash, "A Secure Framework for Protecting Clinical Data in Medical IoT Environment", Smart Healthcare System Design: Security and Privacy Aspects, Wiley, 2022, pp. 203-234.

[10] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, B. Stiller, "Landscape of IoT security", Computer Science Review, Vol. 44, 2022, p. 100467.

[11] M. A. Khan, I. Ahmad, A. N. Nordin, A. E. S. Ahmed, H. Mewada, Y. I. Daradkeh, S. Rasheed, E. T. Eldin, M. Shafiq, "Smart android-based home automation system using internet of things (IoT)", Sustainability, Vol. 14, No. 17, 2022, p. 10717.

[12] R. A. Mouha, "Internet of things (IoT)," Journal of Data Analysis and Information Processing, Vol. 9, No. 2, 2021, pp. 77-101.

[13] C. Komalavalli, D. Saxena, C. Laroiya, "Overview of blockchain technology concepts", Handbook of Research on Blockchain Technology, Academic Press, 2020, pp. 349-371.

[14] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F. Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends", IEEE Transactions on Systems, Man, and Cybernetics: Systems, Vol. 49, No. 11, 2019, pp. 2266-2277.

[15] L. Babun, K. Denney, Z. B. Celik, P. McDaniel, A. S. Uluagac, "A survey on IoT platforms: Communication, security, and privacy perspectives", Computer Networks, Vol. 192, 2021, p. 108040.

[16] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, A. Alazab, "A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks", Electronics, Vol. 8, No. 11, 2019, p. 1210.

[17] D. Guha Roy, S. N. Srirama, "A Blockchain-based Cyber Attack Detection Scheme for Decentralized Internet of Things using Software-Defined Network", Software: Practice and Experience, Vol. 51, No. 7, 2021, pp. 1540-1556.

[18] P. Kumar, G. P. Gupta, R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks", Computer Communications, Vol. 166, 2021, pp. 110-124.

[19] R. M. Qaddoura, A. Al-Zoubi, H. Faris, I. Almomani, "A Multi-Layer Classification Approach for Intrusion Detection in IoT Networks Based on Deep Learning", Sensors, Vol. 21, No. 9, 2021, p. 2987.

[20] J. B. Awotunde, C. Chakraborty, A. E. Adeniyi, "Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection", Wireless Communications and Mobile Computing, Vol. 2021, 2021.

[21] A. A. Hamza, I. T. A. Halim, M. A. Sobh, A. M. Bahaa-Eldin, "HSAS-MD Analyzer: A Hybrid Security Analysis System Using Model-Checking Technique and Deep Learning for Malware Detection in IoT Apps", Sensors, Vol. 22, No.3, 2022, p. 1079.

[22] R. F. Hayat, S. Aurangzeb, M. Aleem, G. Srivastava, J. C. W. Lin, "ML-DDoS: A blockchain-based multilevel DDoS mitigation mechanism for IoT environments", IEEE Transactions on Engineering Management, 2022. (in press)

[23] R. R. Sathiya, S. Rajakumar, J. Sathiamoorthy, "Secure Blockchain Based Deep Learning Approach for Data Transmission in IOT-Enabled Healthcare System", International Journal of Computer and Engineering Optimization, Vol. 1, No. 1, 2023, 15-23.

[24] M. Dhipa, D. Anitha, "Detection of Violence in Football Stadium Through Big Data Framework and Deep Learning Approach", International Journal of Data Science and Artificial Intelligence, Vol. 1, No. 2, 2023, pp. 21-31.

[25] S. Zafar, N. Iftekhar, A. Yadav, A. Ahilan, S. N. Kumar, A. Jeyam, "An IoT Method for Telemedicine: Lossless Medical Image Compression Using Local Adaptive Blocks", IEEE Sensors Journal, Vol. 22, No. 15, 2022, pp. 15345-15352.