International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 12, No.1 (Oct-2022)

https://dx.doi.org/10.12785/ijcds/120172

Enhancement of Blockchain System in Online Transaction by Detecting Attacks Using an Intelligent Approach
Recurrent Neural with Serpent Encryption (RNwSE)

Sk.Khaja Shareef[1], R.Sridevi[2], V. Rama Raju[3] and K. S. Sadasiva Rao[4]

[1]*Research Scholar, CSE Dept, JNTUH &Associate Professor,CSE Dept MLR Institute of Technology Hyderabad.*
[2]*Professor, Computer Science & Engineering, JNTUH College Of Engineering Hyderabad.*
[3]*Professor, Computer Science & Engineering, CMR College of Engineering & Technology Hyderabad.*
[4]*Professor, Department of MCA, Chaitanya Bharathi Institute of Technology, Hyderabad.*

Received 22 Jan. 2021, Revised 15 Jul. 2022, Accepted 23 Jul. 2022, Published 31 Oct. 2022

Abstract: To maintain the security level in any application, implementing the malicious behavior detection approach is crucial. So, the present research work has intended the central concept of malicious behavior detection in the communication medium. In cloud applications, malicious event detection is a complex task because of the extensive unstructured data. The blockchain-based deep network has been introduced to predict malicious behavior to end these issues. Moreover, the detection-based blockchain model is Recurrent Neural with Serpent Encryption (RNwSE). The unknown or malicious characteristics were detected in the initial phase after the homomorphic serpent encryption model functioned. Moreover, we have implemented the planned work in the python frameworks. The scalability of the developed model has been found in terms of encryption-decryption duration and the exactness score of attack detection. Subsequently, the presented paradigm is compared with recently associated schemes and has earned the most satisfactory outcome as high exactness rate and less processing duration.

Keywords: Blockchain, homomorphism, attack detection, large transaction, processing time, security range.

1. Introduction

Blockchain is characterized as a secure and reliable decentralized system in digital innovations [1]. Furthermore, it has involved governments or corporations with collective or individual objectives. After the transaction has been verified, the users have created blocks that comprise a transaction pack and then update to the last block [2]. Furthermore, the data is hidden from unauthenticated users by linking the blockchain with the hash function block [3]. Several blockchain communities networks have recently expressed an interest in organizing machine learning (ML) methodologies to achieve analysis of data or computing statistics findings [4]. Furthermore, medical practitioners building the predictive model for disease diagnosis must offer specialized treatments for individual patients. Moreover, securing cloud-based applications from malicious actions is a critical challenge today in order to improve the cloud computing process [5]. Furthermore, the cloud computing framework has a well-defined encryption technique for securing data. However, a practical attack module may be able to smash the encryption method by compressing the encryption operation or round in some situations [6]. The double-layered encryption strategy poses issues in cloud computing system functioning along with its complexities. Blockchain technology is among the broad perceptions in cloud technology; this blockchain method was initially employed in decentralized systems [7]. As a result, immutability, security, and decentralization are key features of blockchain technology [8]. Before studying homomorphic encryption, cryptographic approaches for securing information in the cloud were more prominent in the previous decade[9].

Furthermore, the cryptographic technique's functionality is based on both asymmetric and symmetric-based encryption. However, it is widely employed in security standards because of its statistical underpinning [10]. Due to the apparent storage space cloud service, several advantages emerge. Operating data in the cloud must require more attention to data authentication and security [11]. Furthermore, cloud data is frequently harmed by many security concerns and attacks. As a result, using a homomorphic encryption strategy in the blockchain context can improve security in the cloud [12]. As a result, homomorphism technology was developed to protect encrypted information

E-mail address: khaja.sk08@gmail.com, sridevirangu@jntuh.ac.in, drvrr@cmrcet.ac.in

in the cloud. Subsequently, the generated homomorphism key is kept in cloud-based storage. The user can verify that the saved data is protected by comparing the own personal hash key to the encoded homomorphism key [13]. Therefore, is if the key gets matched, then the information stored is secure; if indeed the key isn't fit, an attack injects it [14].

A blockchain is just a collection of time-stamped transactions with an odd number of output addresses for each transaction or communication [15]. The goal of the blockchain method is to preserve and protect data integrity. Furthermore, protecting shared data privacy in the cloud becomes critical [16]. Encryption is one method for protecting data or information privacy [17]. Traditional encryption systems require users to decode the encoded information or data to activate it. Traditional cryptography methods are undesirable due to privacy issues [18]. As a result, homomorphic encryption aids in computing information or encrypted data without the need to decrypt it [19]. There was also the option of using an utterly homomorphic encoding approach to execute all operations. However, this experiment cannot be carried out in practice [20]. In addition, various DL (Deep Learning) and ML models exist to protect the data in the blockchain-based environment. Recent techniques like the Crypto-hash procedure [21], TMA [22], BC-DRS[23] , etc., have proposed to stop the issues like attack harmfulness, but still, due to extensive data, the complexity score of attack have recorded. Hence, the present research has aimed to resolve these issues by developing a novel approach with the encryption algorithm.

The research discussion of the current article is organized as follows. The section 2 has detailed the associated works of malicious event detection and blockchain security in various digital fields. The designed novel approach for the discussed problem is detailed in 3th section. Moreover, the robustness of the designed malicious event detection blockchain strategy is summarized in 4th section, and the research discussion and achievements are concluded in section 5.

2. Background

Some recent literatures related to blockchain-based online transactions are described as follows:

Blockchain is the fastest growing technology, which has an important role in the criminal investigation area. P. Velmurugadass et al. [21] have presented a novel method i.e. Cryptographic Hash-based Algorithm (CHA), to monitor activities in a particular area. Initially, based on Authentication Server (AS), all the defined users are registered, and a secret key was obtained from AS by Harmony Search-based Optimization (HSO). Moreover, the result revealed that the presented method had attained better performance concerning the accuracy, throughput, and response time. However, the computational overhead is less.

Parminder Singh et al. [24] have presented a cross-domain-based secure sharing of data platform by multiple-based security gateways. To protect the multiple digital records from different sites the blockchain were used the security keys. Moreover, the blockchain is verified once the application reports the malicious activity. For data transactions and authentication, different algorithms were designed. The result indicated that the presented framework maintains trust. However, this framework is not applicable for large-scale data.

The transaction malleability-based attack (TMA) potential within the application based on blockchain was presented by Kashif Mehboob Khan et al. [22] to determine the settings that led to successful TMA. In particular, TMA successful execution is presented that was carried out on a blockchain-based testbed hosting. The results demonstrated that the presented method has high generating rate of blocks for TMA successful execution and less network delay. Moreover, it does not mitigate against TMA.

Zhili Zhou et al. [23] have proposed a reputation decentralized system in the BlockChain environment; the chosen application to check the working function is online business and education. Moreover, an interplanetary file-based system (IPFS) stores product information such as product comments and descriptions. The presented reputation model has afforded privacy for the communication transmission medium between users. The result indicated that the presented method has desirable reliability and usability.

Mengyao Zhang et al. [25] have presented a Dynamic Data-based Management by Blockchain Model (DDMS-BCM) in a digital economics platform. Moreover, to maintain the privacy lightweight model was studied, and the presented model is readily available in e-commerce by blockchain technologies. The experimental outcome indicated that the presented DDMS-BCM has less decryption and encryption time, high accuracy ratio, and high ratio of data transaction. In addition, the data in the platform are not highly secured.

The key contribution of the current work is described as follows:

- Initially, the online transaction data was collected from the net source and trained to the system
- Then a novel Recurrent Neural with Serpent Encryption (RNwSE) has been designed to protect the data from the malicious events
- Here, the recurrent function is used to predict the present attack during the data transaction
- Once, the attack is predicted then that transmission path is avoided; hereafter the data is transmitted through the other path.

TABLE I. Assessment Literature Survey

Author(s)	Technique	Description/Advantage	Limitation /Research gap
P. Velmurugadass et al.[21]	Cryptographic Hash-based Algorithm (CHA)	Based on Authentication Server (AS), all the defined users are registered, and a secret key was obtained from AS by Harmony Search-based Optimization (HSO).	The computational overhead is less
Parminder Singh et al. [24]	cross-domain-based secure sharing of data platform by multiple-based security gateways	Protects the multiple digital records from different sites the blockchain were used the security keys.	This framework is not applicable for large-scale data.
Khan et al. [22]	The transaction malleability-based attack (TMA)	TMA successful execution is presented that was carried out on a blockchain-based testbed hosting. The results demonstrated that the presented method has high generating rate of blocks for TMA successful execution and less network delay.	It does not mitigate against TMA.
Zhili Zhou et al. [23]	A reputation decentralized system in the Blockchain environment	The presented reputation model has afforded privacy for the communication transmission medium between users.	An interplanetary file-based system (IPFS) stores product information such as product comments and descriptions.
Mengyao Zhang et al. [25]	Dynamic Data-based Management by Blockchain Model (DDMS-BCM) in a digital economics platform	The presented DDMS-BCM has less decryption and encryption time, high accuracy ratio, and high ratio of data transaction.	The data in the platform are not highly secured

- Finally, the proficiency of the proposed model is estimated in terms of encryption time, data transmission...etc

A. SYSTEM MODEL AND PROBLEM DESCRIPTION

As discussed in the previous publications, there is numerous detection mechanisms were implemented in blockchain strategy. But, due to the data vastness and complexity, the detection mechanism has resulted in poor performance. Moreover, the inefficient detection approaches have needed maximum resources and duration to complete the process. Also, in some cases, the malicious activities have been detected wrongly that has tended to attain high data and resource loss. Also, the cloud transaction system was too large, so forecasting the malicious events is not all a simple task. Hence, the detection mechanisms based on deep networks were implemented with suitable parameters to end these issues. The blockchain system with detection problems are illustrated in fig.1.

3. PROPOSED RNWSE FOR ATTACK DETECTION BLOCKCHAIN SYSTEM

This research aims to improve the services of blockchain systems by enabling the deep networks-based attack vulnerabilities prediction model. Consequently, the planned approach is named a novel RNwSE model. Hence, the recurrent function is utilized along with the holomorphic-serpent model. To validate the detection performance of the developed scheme, some malicious characters were launched in the data transaction model. The detection parameter of the recurrent networks has been activated to identify the abnormal features present in the communication channel.

The interest towards deep recurrent networks is for better prediction results. The recurrent networks have been utilized in various platforms and have earned a better prediction exactness value than other intelligent models. The proposed framework and function steps are elaborated in Fig.2.

A. Layer design of Proposed RNwSE

The planned design has five phases: input layer, error pruning or preprocessing phase, classification phase, detection parameter updating phase, and output layer. Those functions were activated before the blockchain process. Because hiding the original data with malicious events is complicated, it has attempted a less confidential score. Moreover, the proposed novel RNwSE has been created

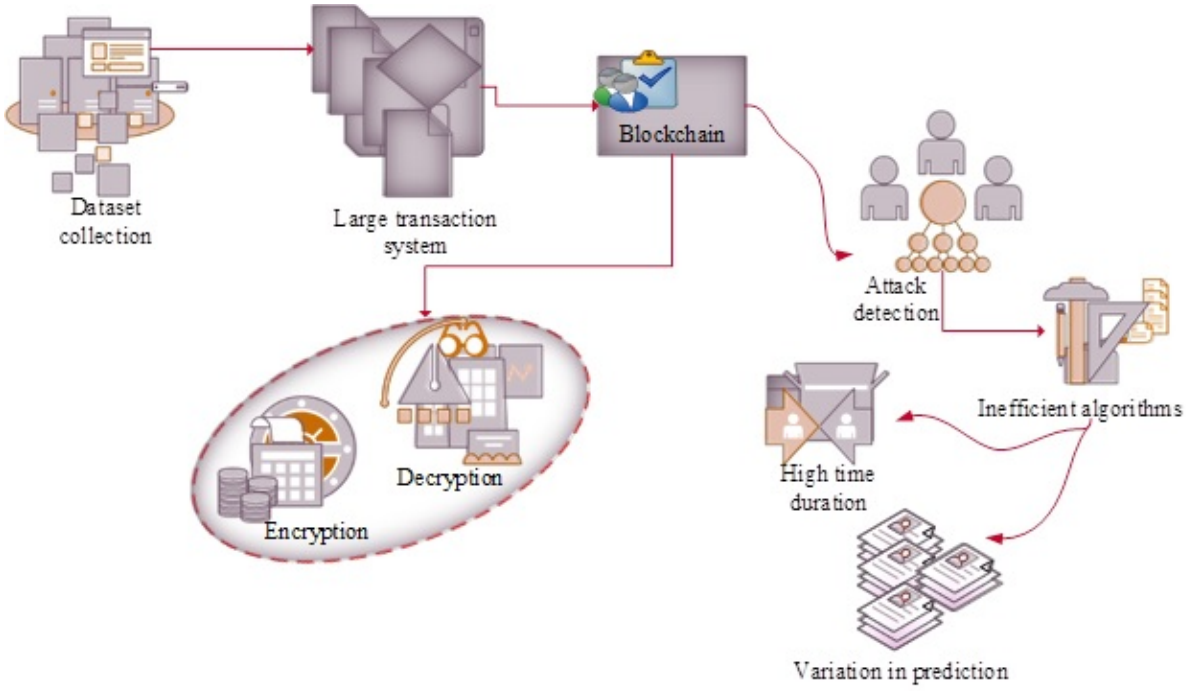


Figure 1. Attack detection module in blockchain

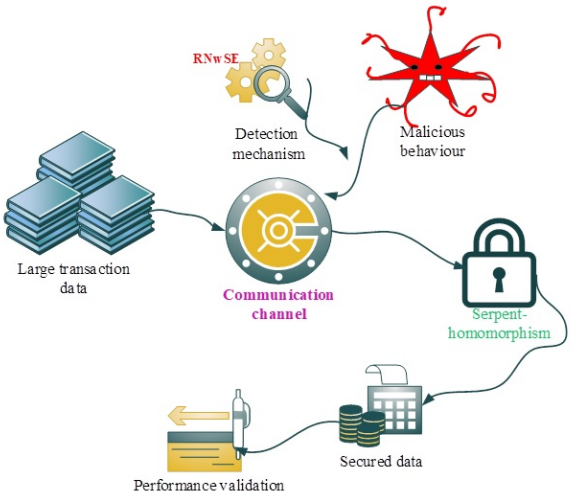


Figure 2. Proposed RNwSE architecture

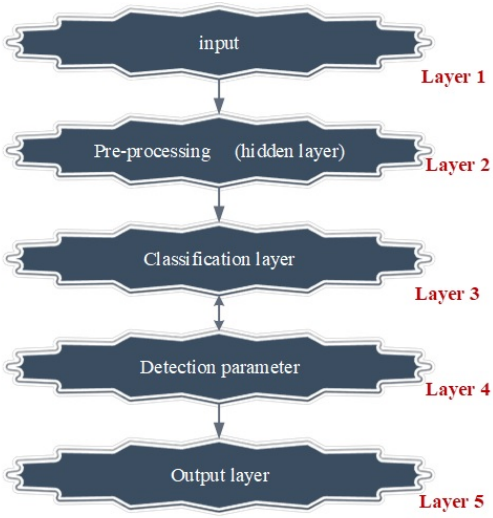


Figure 3. layers of RNwSE

with recurrent functions [26] and the serpent model [27].

$$i_t = a_f(Bpt + C_m i_t + b) \quad (1)$$

The time series function of the recurrent network was determined as i_t, B, C are the weight function, vector variable is denoted as p and af is represented as activated function. Moreover, m denoted the matrices, which described the weight function has executed in matrix form. Hence, the training function is processed by Eqn. 1. The layer of the novel RNwSE is detailed in Fig.3.

1) Preprocessing

To get the refined data, the process preprocessing has performed for the trained datasets. Mostly, the raw data from net sources contains some noise features. Processing the data without cleaning has earned very less outcome, so error extraction function has processed with suitable and

possible parameters.

$$l_t = f_f + n_f \tag{2}$$

Where, large transaction trained dataset is denoted as l_t, fresh features are represented as f_f and noisy contents are determined as n_f. Hence, the eqn.2 has detailed that the imported data includes both noisy and fresh features.

$$Pr(n_f) = l_t - n_f \tag{3}$$

Moreover, pruning functions of the noise features are measured using Eqn.3. After the error removal function, the error-cleared dataset has been attained.

2) Feature analysis and malicious events prediction

Predicting malicious and normal events is done using the if condition statements described in eqn.(4). Where the feature analysis variable is determined as Ea

$$Ea = \begin{cases} if user = 0 & normal \\ if user \neq 0 & abnormal user \end{cases}$$

The concept obtained for the detection purpose is the deep neural model, so training and testing of the data are in the form of 0 and 1. Here, in class 0 the normal behaviors have been stored, and in-class "1" malicious characteristics have been stored.

3) Serpent homomorphic encryption

Serpent crypto approaches were influenced by current ideas for implementing ciphers using bit-slices. The function that has been incorporated in the serpent model is bit-slicing. It has taken a few seconds to encrypt each block of data than other crypto models. This enables the utilization of standard modes of operation, which eliminations the need to alter the rapidity environment to achieve the additional speed.

$$Se = l_t + k(XOR) = L_T \tag{4}$$

Here, the encryption parameter is represented as Se and k is key. Moreover, L_T is the encrypted data that is elaborated in eqn.4. Then to perform the homomorphic process, the encrypted data L_T is taken into consideration that is equated in eqn. (6)

$$H = l_T(hash function) \tag{5}$$

If the hash value is calculated for the encrypted data, it is verified with the initial hash value. If two has values are matched during the verification process, then files or insecure conditions. The steps to execute the novel RNwSE paradigm are detailed in algoritm.1 and Fig.4.

4. RESULTS AND DISCUSSION

The planned detection-based blockchain strategy is executed in the python environment, windows 10 platform, and the scalability score of the proposed RNwSE has been analyzed by performing the detection process for the large transaction data. Also, the stability of the presented model is validated for the different data sizes. The execution parameters are discussed in table.II.

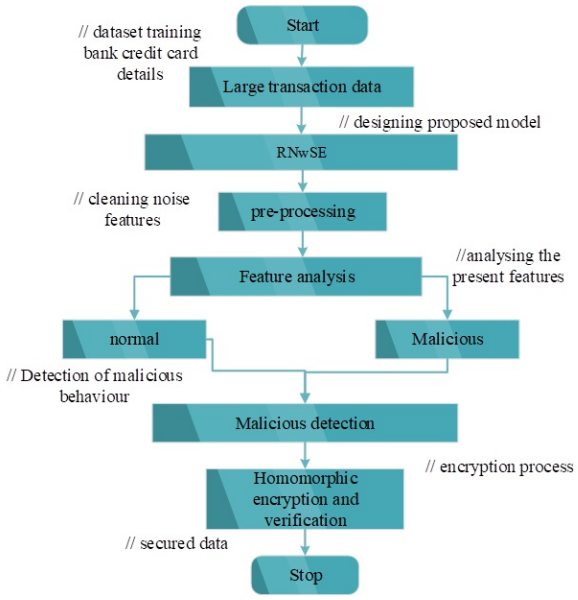


Figure 4. Proposed RNwSE flow model

TABLE II. Execution parameter constraints

Parameter	Specification
Platform	python
Operating system	Windows 10
dataset	Large transaction data
Training methods	Recurrent deep networks
technology	Blockchain
parameters	• Encryption time • Hash generation time • Decryption time • Attack detection accuracy
Attack type	DoS
Attach counts and names	• Attack count 3 • slowloris • packet flooding • ping-of-death

A. Case study

To validate the function of the created novel RNwSE, a large bank transaction data has been taken. Moreover, those data include both normal and malicious behavior; all features were trained to the system in the initial phase and stored separately in the memory frame of the recurrent model. The internal system of RNwSE is drawn in fig.5. During the process of testing, some user behavior has been imported, and the detection function of the RNwSE has been measured in case of accuracy and confidential score. In addition, the robustness value of the designed RNwSE is measured with the presence of a DoS attack. Actually, the DoS is the most deadly attack in wireless or network channels; if the DoS malicious event is present in the communication medium, it interrupts the entire system performance by flooding the packets. In addition, three kinds of DoS attacks has been checked the designed deep

Algorithm 1 RNwSE

```
procedure START
    int i_t,a_f
    procedure PRE-PROCESSING MODEL                    ▷ activating the recurrent function
        int pr,n_f,f_f                                ▷ initiating pre-processing variable
        pr(n_f(l_t)) → L_T                            ▷ error-less data has been obtained
    end procedure
    procedure FEATURE ANALYSIS AND MALICIOUS FEATURE DETECTION
        int Ea                                        ▷ feature analysis parameter
        Ea → analysis(0,1)                            ▷ analyzing the normal and malicious features
    end procedure
    procedure MALICIOUS BEHAVIOR DETECTION
        if user=0 then
            Normal user behavior
        else
            Malicious behavior                        ▷ finally malicious behavior has been identified
        end if
    end procedure
end procedure
```

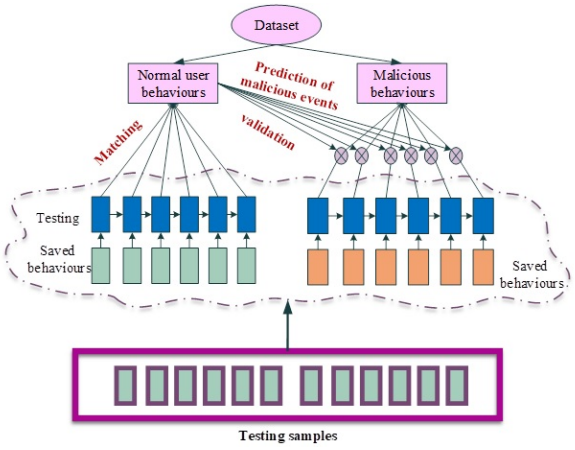


Figure 5. Interior work process of RNwSE

TABLE III. Type of attack and detection metrics

Attack prediction assessment		
DoS types	Accuracy of detection	Detection time
Slowloris	98	2ms
Packet flooding	98.1	5ms
Ping of death	98.01	3ms

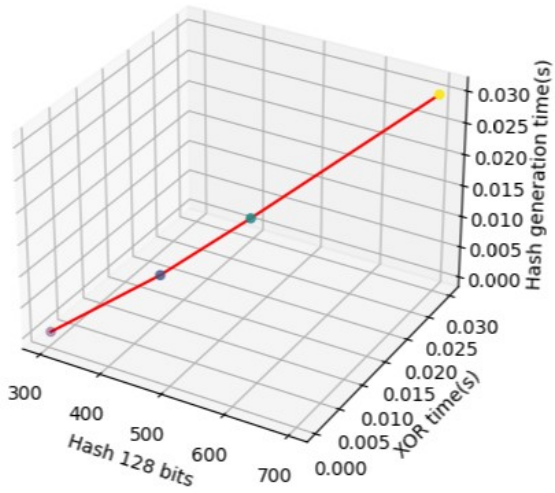
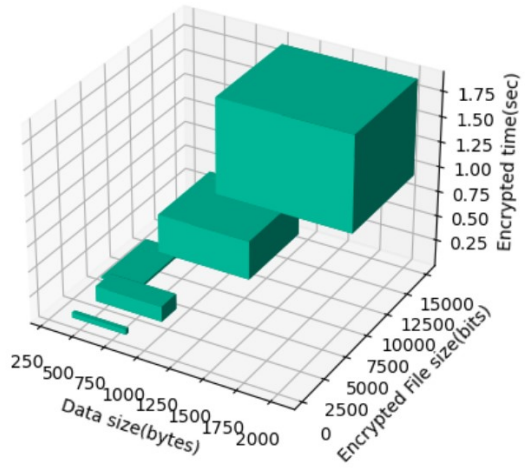


Figure 6. Hash assessment

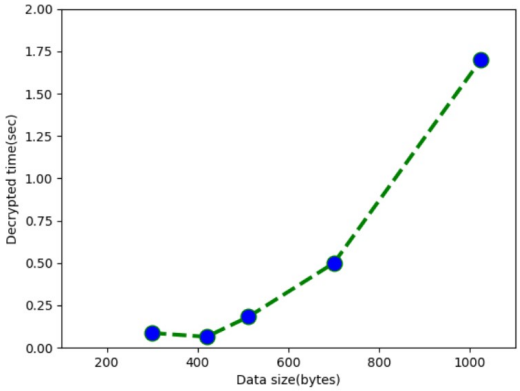
TABLE IV. Hash calculation details

hash 128 bits	Serpent homomorphism	
	XOR time(s)	Hash Generation time(s)
300	0.0005	0.0005s
420	0.008	0.008s
512	0.015	0.015
700	0.03	0.03s

network-based blockchain system; those results are tabulated in table.III. The encryption process has been validated in three cases: time taken for encryption, encrypted file size, and original file size. Those details are shown in 3D graphical representation fig.6 and table.IV. Also, in crypto models, the hash function is the initial key steps to high the data from the third parties before the encryption is done. Here, the initial hash is generated serpent model with the help of XOR functions. If it was created then it has been saved in the cloud location. Consequently, if anyone need to retrieve the data grant access procedure has performed that is verification process of dual hashes. For 300bytes data, the XOR and hash measure time taken by homomorphic serpent model is 0.0005s. Also, the time taken by 420 bytes data for hash and XOR duration is 0.008s. In addition, the recorded hash and encryption time for 512 bytes data is 0.15s. Finally, for the 700 bytes data



(a)



(b)

Figure 7. Encryption assessment: a)encryption time and file size, b)decryption time

the required duration for hash and data encryption time is 0.03s. Here, the decryption duration is higher than the encryption; this proves the encrypted data is more secured with a high confidential rate. The size of the considered original data is 300 bytes; after the encryption process, the size of the file is reduced up to 4857 bits. The time take for the encryption function is 0.02s, and the decryption duration is 0.087s. For 420 bytes of original data, the duration for encryption is 0.052s, and decryption is 0.065s. Also, the size of the encrypted data is 2564 bits. For 512 bytes of original data, the time required for encryption is 0.15s and decryption is 0.183s also, the size of the encrypted data is 1549 bits. In addition, for 700 bytes data, the encrypted data volume is 5735 bits, encryption period 0.95s and decryption duration 0.5s. Finally, for 1MB data, the encrypted file quantity is 7525 bits, encryption time 0.95s and 1.7s for decryption; these statistics are detailed in fig.7.

B. COMPARISON ASSESSMENT

In the blockchain concept, measuring time is very important. Hence, the time form encryption and decryption functions have been validated with various sizes of data bytes. In addition, for the comparison, certain methods have been obtained that are Long-Short-term-Approach (LSTA) [28], dual-level privacy (DLP) [28], and data Aggregation (DA) [29].

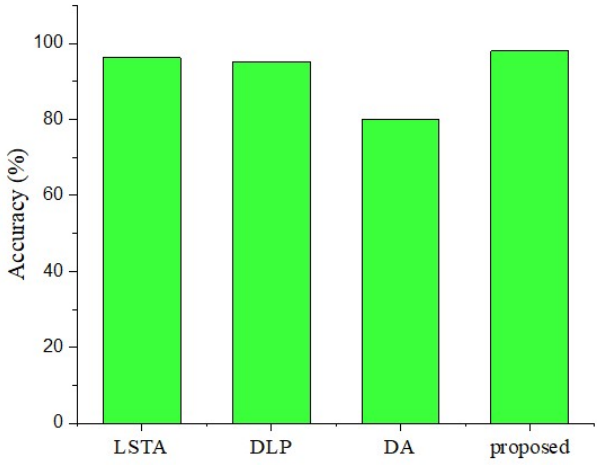


Figure 8. Accuracy validation

1) Accuracy Assessment

In this present work, the key metrics are accuracy and expected duration. Hence, the accuracy and overall time consumption have been elaborated. Hence, the exactness rate is measured by Eqn.6.

$$accuracy = \frac{detectedmaliciousbehavior}{Totalbehavior} \quad (6)$$

The metric accuracy is a measure to calculate the exactness score of malicious events detection in all aspects. But, if the communication channels were increased, there would be little loss in exactness rate. Here, the method LSTA has obtained 96.27% accuracy, DLP has observed a 95.27% exactness rate, and DA has 80% accuracy. Besides, the present approach has earned a better prediction exactness rate of 98%. Those values are graphically detailed in fig.8.

2) Processing time

In cloud application evaluating time concern is the chief metric to value the successive score of the applied models. Hence, the metrics processing duration has been measured.

Here, the technique LSTA has obtained the processing duration as 73s, the model DA has yielded 20s to execute the process, and the serpent-blockchain has recorded 25s to complete the process. Considering all method, the designed detection-based blockchain concept has recorded 12s to complete the one run. Comparing all methods, the proposed RNwSE has reported less execution duration. Moreover, discussed statistics are detailed in fig.9.

C. Discussion

The designed RNwSE approach has earned the finest outcome from overall performance measurements. It has

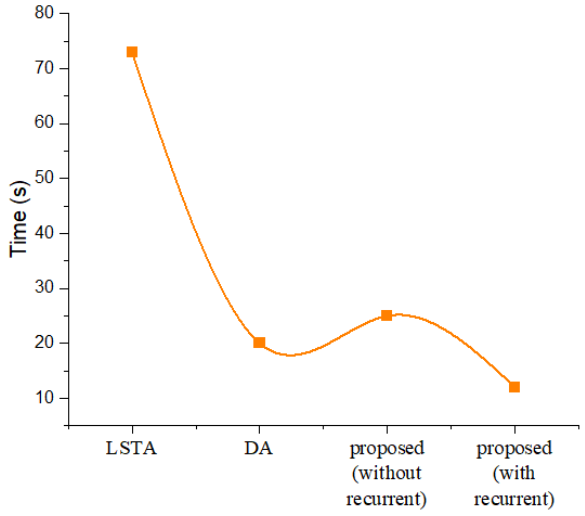


Figure 9. Processing time validation

TABLE V. Overall RNwSE assessment

	Encryption assessment		Decryption	Detection accuracy
Data Size (bytes)	File Size (bits)	Time	Time	
300	4857	0.02	0.087	98
420	2564	0.052	0.065	97.8
512	1549	0.15	0.183	97.5
700	5735	0.38	0.5	97
1MB	7525	0.95	1.7	96.9

verified that a novel RNwSE has suitable for the blockchain field in predicting the malicious behaviors from the total user characteristics. The overall function of the RNwSE approach is detailed in the table.V. Moreover, the main advantages of this investigation are the proposed novel RNwSE model is analyzed for different sizes of data and different DoS attacks. But the only demerits are the absence of the monitoring model for all time. So there is the possibility of the attack vulnerabilities after some specific time. So implementing the continuous monitoring system with the homomorphic serpent blockchain concept will improve the performance and gain the finest confidential results.

5. Conclusions and Future Work

The current article has implemented a novel RNwSE as the malicious detection model for the digital blockchain system. Hence, malicious behavior detection has been carried out on large transaction datasets. Subsequently, types of DoS attacks have been launched in the designed blockchain framework to verify the robustness score of the presented detection model. Moreover, the proposed novel RNwSE has gained 98% accuracy for malicious behavior detection. Hence, it has improved 2% of detection accuracy than the previous models. During the validation, it has scored very less duration as 12s to complete the process; when compared to another model, it has minimized the processing duration up to 10s. Also, in all cases of attack launching models, the blockchain system has been remained secure in a stable range. In the future, implementing the continuous monitoring model with the help of heuristics and deep features will provide the better security rate.

References

[1] A. Banotra, J. S. Sharma, S. Gupta, S. K. Gupta, and M. Rashid, "Use of blockchain and internet of things for securing data in healthcare systems," in *Multimedia Security*. Springer, 2021, pp. 255–267.

[2] U. Majeed, L. U. Khan, I. Yaqoob, S. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for iot-based smart cities: Recent advances, requirements, and future challenges," *Journal of Network and Computer Applications*, vol. 181, p. 103007, 2021.

[3] M. Zia, "B-drive: A blockchain based distributed iot network for smart urban transportation," *Blockchain: Research and Applications*, vol. 2, no. 4, p. 100033, 2021.

[4] D. Li, Z. Luo, and B. Cao, "Blockchain-based federated learning methodologies in smart environments," *Cluster Computing*, pp. 1–15, 2021.

[5] P. Sharma, S. Jain, S. Gupta, and V. Chamola, "Role of machine learning and deep learning in securing 5g-driven industrial iot applications," *Ad Hoc Networks*, vol. 123, p. 102685, 2021.

[6] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain-based decentralized architecture for cloud storage system," *Journal of Information Security and Applications*, vol. 62, p. 102970, 2021.

[7] B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, "Unification of blockchain and internet of things (biot): requirements, working model, challenges and future directions," *Wireless Networks*, vol. 27, no. 1, pp. 55–90, 2021.

[8] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, and Z. Zou, "A blockchain-based architecture for secure and trustworthy operations in the industrial internet of things," *Journal of Industrial Information Integration*, vol. 21, p. 100190, 2021.

[9] H. Yousuf, M. Lahzi, S. A. Salloum, and K. Shaalan, "Systematic review on fully homomorphic encryption scheme and its application," *Recent Advances in Intelligent Systems and Smart Applications*, pp. 537–551, 2021.

[10] M. Muhammad and G. A. Safdar, "5g-based v2v broadcast communications: A security perspective," *Array*, vol. 11, p. 100084, 2021.

[11] T. Wang, Y. Quan, X. S. Shen, T. R. Gadekallu, W. Wang, and K. Dev, "A privacy-enhanced retrieval technology for the cloud-assisted internet of things," *IEEE transactions on industrial informatics*, 2021.

[12] H. Xie, Z. Zhang, Q. Zhang, S. Wei, and C. Hu, "Hbrss: Providing high-secure data communication and manipulation in insecure cloud environments," *Computer Communications*, vol. 174, pp. 1–12, 2021.

[13] H. He, R. Chen, C. Liu, K. Feng, and X. Zhou, "An efficient ciphertext retrieval scheme based on homomorphic encryption for multiple data owners in hybrid cloud," *IEEE Access*, vol. 9, pp. 168 547–168 557, 2021.

[14] P. Kar, S. Misra, A. K. Mandal, and H. Wang, "Sos: Ndn based service-oriented game-theoretic efficient security scheme for iot networks," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3197–3208, 2021.

[15] H. Honar Pajooh, M. A. Rashid, F. Alam, and S. Demidenko, "Iot big data provenance scheme using blockchain on hadoop ecosystem," *Journal of Big Data*, vol. 8, no. 1, pp. 1–26, 2021.

[16] A. Qashlan, P. Nanda, X. He, and M. Mohanty, "Privacy-preserving mechanism in smart home using blockchain," *IEEE Access*, vol. 9, pp. 103 651–103 669, 2021.

[17] Y. Yang, F. He, S. Han, Y. Liang, and Y. Cheng, "A novel attribute-based encryption approach with integrity verification for cad assembly models," *Engineering*, vol. 7, no. 6, pp. 787–797, 2021.

[18] K. Halunen and O.-M. Latvala, "Review of the use of human senses and capabilities in cryptography," *Computer Science Review*, vol. 39, p. 100340, 2021.

[19] R. Abid, C. Iwendi, A. R. Javed, M. Rizwan, Z. Jalil, J. H. Anajemba, and C. Biamba, "An optimised homomorphic crt-rsa algorithm for secure and efficient communication," *Personal and Ubiquitous Computing*, pp. 1–14, 2021.

[20] B. Li and D. Micciancio, "On the security of homomorphic encryption on approximate numbers," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2021, pp. 648–677.

[21] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, "Enhancing blockchain security in cloud computing with iot environment using ecies and cryptography hash algorithm," *Materials Today: Proceedings*, vol. 37, pp. 2653–2659, 2021.

[22] K. M. Khan, J. Arshad, and M. M. Khan, "Empirical analysis of transaction malleability within blockchain-based e-voting," *Computers & Security*, vol. 100, p. 102081, 2021.

[23] Z. Zhou, M. Wang, C.-N. Yang, Z. Fu, X. Sun, and Q. J. Wu, "Blockchain-based decentralized reputation system in e-commerce environment," *Future Generation Computer Systems*, vol. 124, pp. 155–167, 2021.

[24] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Cross-domain secure data sharing using blockchain for industrial iot," *Journal of Parallel and Distributed Computing*, vol. 156, pp. 176–184, 2021.

[25] M. Zhang, L. Lin, and Z. Chen, "Lightweight security scheme for data management in e-commerce platform using dynamic data management using blockchain model," *Cluster Computing*, pp. 1–15, 2021.

[26] J. C.-W. Lin, Y. Shao, Y. Djenouri, and U. Yun, "Asrnn: a recurrent neural network with an attention model for sequence labeling," *Knowledge-Based Systems*, vol. 212, p. 106548, 2021.

[27] H. T. Elshoush, B. M. Al-Tayeb, and K. T. Obeid, "Enhanced serpent algorithm using lorenz 96 chaos-based block key generation and parallel computing for rgb image encryption," *PeerJ Computer Science*, vol. 7, p. e812, 2021.

[28] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K.-K. R. Choo, "A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5110–5118, 2019.

[29] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," *Computers & Electrical Engineering*, vol. 93, p. 107209, 2021.

Sk.Khaja Shareef is a research scholar at Jawaharlal Nehru Technological University Hyderabad, Telangana in the area of Information Security and he is working as assistant professor in MLR institute of Technology. He received his B.Tech. in Information Technology from Kakatiya University and M.Tech in Information Technology from JNTU Hyderabad. Presently, he is working as Associate Professor in the department of IT at MLR institute of Technology, Hyderabad, Telangana. He is having a good number of publications in reputed journals.

Dr. R Sridevi received her B.Tech from Madras University, Chennai in Computer Science and Engineering and M.Tech in Computer Science and Engineering from Andhra University, Andhra Pradesh and PhD in CSE from JNTUH College of Engineering Hyderabad. She has around 16 years of teaching experience from JNTUHCEH. She works as Professor in CSE & Coordinator, Centre of Excellence in Cyber Security, JNTUH College of Engineering Hyderabad, India. She has published more than 20 papers in refereed journals and conference proceedings. Her research interests include Computer Networks, Information Security, and Network Security.

Dr. K. S. Sadasiva Rao received his PhD from JNTUH Hyderabad, in Computer Science and Engineering He has around 20 years of teaching experience from reputed Engineering Institutions. He working as Professor in the MCA Department, Chaitanya Bharathi Institute of Technology, Hyderabad, India. He has published more than 20 papers in refereed journals and conference proceedings. His research interests include working as Professor in the MCA Department, Chaitanya Bharathi Institute of Technology, Hyderabad.

Dr. V. Rama Raju received his Post-B.Tech from Central University of Hyderabad (HCU), in Computer Science and Engineering and M.Tech in Computer Science and Engineering from JNU New Delhi and PhD in Neurology & Biomedical Engineering from Nizam‘s Inst of Medical Sciences (NIMS) University Hyderabad. He has around 35 years of teaching experience from reputed Engineering Institutions. He working as Professor in the CSE Department, CMR College of Engineering Hyderabad, India. He has published 3 books and more than 200 papers in refereed journals and conference proceedings, having 300 citations. His research interests include Computer Science & Engineering/ Information Technology Currently working on wireless sensor – Vehicular Adhoc Networks.

Artificial Intelligence-Computational & Cognitive system, AI, Natural Language Speech & Auditory Processing, Machine Translation, Lexical computation, specification design & devt of computational lexicon & Neuro-Linguistics, Pattern Recognition & feature extraction Biomedical Engineering – Biomedical Instrumentation and Signal Processing and Multichannel Electrode Recordings (Micro, surface, induced, intramuscular, intra/extra cellular microelectrodes) Neuroscience - Neurology/Functional Neurosurgery – Neurodegenerative Parkinson‘s Disease/ MER with DBS Electrode Implantation in PDs, Dystonia Writer‘s Cramp and other Movement Disorders, Neuromuscular diseases, Cognitive science Biomedical Signal processing-Neuro-Muscular Human Motor Control system, EMG Writer‘s and Musician‘s Cramp, Dystonia.