ISSN: 2633-4828 Vol. 5 No.4, December, 2023

International Journal of Applied Engineering & Technology

A BLOCKCHAIN WITH SHA-256 ALGORITHM FOR INTRUSION DETECTION TO ENHANCE SECURITY

Mrs. Abirami.K[1] and Dr. Jasmine Samraj[2]

[1]Research Scholar (Ph.D), PG & Research Department of Computer Science, Quaid-E-Millath Government College for Women (Autonomous), Chennai

[2]Associate Professor,Research Supervisor, PG & Research Department of Computer Science, Quaid-E-Millath Government College for Women (Autonomous), Chennai

[1]abiramik.research@gmail.com and [2]dr.jasminesamraj@qmgcw.edu.in

ABSTRACT

In the past few years, cyberattacks have grown more intricate and advanced. Network security has increased with the advent of the Internet of Things and the digital revolution. Commonly used technologies to secure networks are intrusion detection and prevention systems. One of the information technologies that is safely gaining traction and helps to secure data is blockchain. Blockchain technology protects data against cyberattacks. User data is increasingly secure because once it is initialised by the user, it cannot be changed or transferred. Since user information is unable to be exchanged with illegal or authorised persons on the network other than those now using it, privacy of information is unaffected. This study compares the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption algorithms for identifying intrusions with a block chain using the SHA-256 algorithm. Specifically, this outlined the intrusion detection using blockchain, talk about how blockchain can be used for intrusion detection, and point out unresolved issues in this area.

Keywords: Internet of Things, SHA-256, blockchain, intrusion detection, AES , RSA.

I. INTRODUCTION

The sophistication of hacking has increased recently, and hackers who propagate via the network have a significant negative influence on community. Although it is extremely hard to totally prevent such risks, identifying them in the beginning may assist shield the systems from attack. Consequently, intrusion detection systems (IDS) are employed to lessen network risk. Compared to cables, wireless networks are more susceptible to fraudulent attempts. IDS are primarily designed to track and examine traffic across networks and identify various types of threats that are launched against the network.

The enhanced surveillance effectiveness of intrusion detection platforms has led to their growing popularity and implementation in many companies; yet, two significant problems persist: credibility computing and data interaction. In the beginning, not all participants want to expressly reveal their knowledge, which makes the exchange of data a significant issue for simultaneous identification. To construct typical identities, for instance, finding anomalies frequently uses machine learning methods; for this purpose, a classifier needs a lot of training data. It is challenging to optimise the accuracy of detection since a few organisations are reluctant to disclose their data due to issues of privacy. Furthermore, internal assaults pose a significant threat to coordinated discovery and can seriously weaken the safety of networks. Therefore, in a decentralised and collaborative setting, it can be difficult to determine whether an IDS node is reliable. For example, it is difficult to measure the credibility status of multiple participating entities accurately.

In the field of intrusion detection, novel methods are required to meet the issues mentioned above. The innovative nature of blockchain technology which enables mutually distrusting entities to communicate monetary information without the assistance of a third party has drawn a lot of interest from universities and businesses in recent years. This is the ideal characteristic for intrusion detection, providing an opportunity to address issues with transferring information and trustworthiness.

The liberty users are granted to read and write on the record, i.e., whether they allow public or restricted access for reading as well as permissioned or free access for writing and establishing agreement, define the structure of a blockchain. There are three different blockchain topologies to be aware of:

1. A public, permissionless blockchain that allows anybody to read, write, and reach consensus on any topic. Although some degree of anonymity or pseudo-anonymity is used by those involved, the exchanges are visible.
2. Private permissionless blockchain: Contributing nodes need to be invited or granted authorization to enter the network in order to take part in agreement or execute activities on the distributed database. Different systems for controlling access could be used, such as a group of people making the decisions, a governing body issuing membership permits, or current participants selecting prospective recruits.
3. The Sovrin Foundation established the concept of public permissioned blockchain, which characterises blockchain versions that are open to the people. This implies that anybody can read or modify the ledger's state, while the number of nodes that reaches consensus is restricted. When adopting this kind of blockchain, the ledger can only be edited by a chosen group of people.

APPLICATION OF BLOCKCHAIN IN IDS

It has been shown in recent years that attackers are utilising more sophisticated and innovative techniques to infiltrate networks covertly. Furthermore, it is probable that the network administrator's focus will be diverted if there is any errors or hacking on the network. Because so many IDSs are linked to the consolidated server, there is a significant problem with the validity of the logs and warnings generated by the various IDSs.

II.RELATED WORK

Shitang Yu et al.[6] [In this study, a Powerful Blockchain System featuring the PBFT-DPOC consensus formula and distributed system for networks were developed. In this section the researchers suggested a three-layer design: the DAPP level, the blockchain level, and the sophisticated instrument level, to achieve safety and effectiveness for the node-to-node representation that connects intelligent gadgets.A number of investigators are currently focusing on encryption scheme designs based on the technology of blockchain; some of these are covered in this part of the paper. In this study, the authors show how to employ the blockchain approach in attack detection systems (IDSs) to safeguard user information. Blockchain technology is used in cloud computing design to create a secure user experience. A blockchain network does not concentrate on a single data centre or server; instead, it spreads resources such as interconnections.

M. Baza et.al [8] This article suggests a novel ABE technique for safely renting out decryption that makes use of blockchain knowledge. In the suggested architecture, an intelligent contract is employed to validate the payment made to the other corporation in the event that the contracted decoding procedure is successful. In order to allow users to confirm the accuracy of the decryption result, it also uses the sampling approach. Conversely, the suggested approach utilises the ABE method to guarantee solely the secure outsourcing decryption procedure, rather than the revocation technique.

A. Ruggeri et.al [9] The deployment of blockchain for the Internet of Things and preserving privacy in businesses provide numerous technical challenges that are examined in this article. Despite the challenges, blockchain systems show great potential to address privacy, safety, and credibility concerns in multi-stakeholder projects.

R. V. Biradar et.al [10] In this study, the Qlearning method is presented. It is used to estimate nodes' trustworthiness based on previous communications and to learn the node's present condition, including location and speed. The procedure known as PSO is used to place nodes containing sensors in the network in a way that maximises protection, interaction and durability, and utilisation of energy. Moreover, the method known as AES

uses the most effective fitness quality, or the best possible outcome derived by PSO, to choose keys for encryption.

A. K. Mishra et.al [11] Autonomous cars (AVs) were developed to facilitate everyday activities by transporting cargo, delivering parcels, and reducing traffic. The applications for the unmanned vehicles were very broad and included undersea instruments, cars, and aircraft. They established the Cyber Security (CS) facilitated transmission of information for self-driving vehicles in order to make the problem easier to solve. A network functions as the intermediary, transferring information of the transmitter to the driverless vehicle. For extra security, the CS dependent technique known as the Advanced Encryption Standard, or AES, is used to unlock the information, which is convertible to encrypted code. With the private key that the broadcaster provides to the unique AV, encrypted data may be decoded. An ordinary neural system would be altered using modified particle swarm performance. The ultimate goal of the researchers' suggested product should be to use double cryptography to reveal the work.

S. Sankaranarayanan et.al [12] These days, due to its features, Mobile Ad Hoc Networks are a popular study topic. Mobile Ad Hoc Networks typically provide handheld devices with inadequate safety measures. There is a high probability that hackers will target the function's host nodes due to this issue. It is possible to identify attackers before they have a chance to attack nodes by using malware detection methods. The initial layer of defence for security in a MANET is thought to be the intrusion detection system (IDS). The author explains a public RSA algorithm-based security detection method.

M. Sabarish et.al [13] In this paper, the use of deep learning Trusted Safe Attacker Identification (IDLTSAD)-based framework for detection of breaches, safety and energy conservation is proposed. Using IDLTSAD has many advantages, the most significant being longer network lifespan and enhanced security. The data encryption method used by SDN was intended to be utilised in tandem with this cryptographic safety technology. Since it included an attribute-based cryptography (ABE) system, this approach is trustworthy.

S. Sujitha et.al [14] In the context of cloud structures, this study suggests an approach to detect and reduce unnecessary traffic and messages, especially repeated ones. Building an Intrusion Finder and Analytical device platform which allots extra capacity and safely saves user data is the process. In order to identify inappropriate behaviour, the system checks the individual file dimensions of received documents with their initial versions; any differences are reported as potential DDoS attacks. For further transfer of data, the RSA encryption technique is used for higher safety.

P. K. Naik et.al [15] In the context of cloud settings, this study suggests an approach to detect and reduce unnecessary traffic and messages, particularly duplicate ones. The method necessitates building an IntrusionFinder and Sensor (IF-AD) structure, which spreads backup files and securely maintains user data. This method compares the original file sizes with the sizes of those downloaded to look for differences that can indicate a potential distributed interruption of service assault (DDoS).

X. Zhan et.al [16] The block chain network surveillance system is examined in this study. First, a brief introduction of block chain's features is given, followed by a proposal of the safety and privacy issues with block chain networks. Furthermore, the WLAN detection system for intrusions was created by experimentation. The block chain network surveillance system's outcome review is ultimately covered.

M. Kumar et.al [17] This study suggests building a Distributed attack detection system (DIDS) on a solid foundation such as the cloud, while utilising cutting-edge and exciting developments like blockchain.

W. Liang et.al [18] This study provides an integrated clustering-characteristic-based data integration method for detecting breaches in a Blockchain-based network. Data groups in the networks of Blockchain are trained and evaluated using a machine learning algorithm, and a theoretical framework of information fusing is constructed. The aberrant qualities in a Blockchain collection of data are identified, an unbiased analysis is carried out, and the

cumulative ratings across many nodes are computed following multiple rounds of cooperative interaction between the aggregating nodes.

G. Gurung et.al [19] This study proposes a CIDSs design that utilises Hyperledger Fabric and Snort IDS, and investigates how the use of Blockchain might improve the resilience and effectiveness of CIDSs when it comes to handling trust.

II.Advanced Encryption Standard (Aes)

One popular method of encryption that is used for cryptography is AES. AES has a distinct encryption and decryption system of its own.Each of the three key lengths that AES can handle—AES 128 bit, 192 bit, and 256 bit—has a block size of 128 bits. The key length determines how many rounds there are. AES employs 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. The amount of rounds depends on the size of the key.

III.Rivest-Shamir-Adleman (Rsa)

It is among the most renowned cryptosystems with public keys for data block encoding, electronic signatures, and transfer of keys. RSA uses an adjustable length encoding block and configurable length key. Heterogeneous (publicly accessible key) encryption based on the concept of numbers is used in this block crypto scheme. Two prime values are employed for creating the keys for both public and private use. Each of these unique keys are employed in both encryption as well as decryption. A communication is encrypted by the sender using the receiver's freely accessible key, which the recipient can decrypt using his own password.Key creation, encrypting data and decoding are the three main phases that make up an RSA function. Because of its numerous shortcomings in design, RSA is not recommended for use in businesses. The encryption method becomes inadequate when tiny amounts of p and q are chosen for the key design, and attacks using side channels and random probability theory can be used to decode the data. On the other hand, in comparison with DES, selecting lengthy p & q lengths causes processing times to increase and efficiency to decrease. Furthermore, the procedure requires that p and q have the same sizes, and this presents a particularly hard condition to satisfy in real life. When these situations arise, the system's expenses increase because padding strategies take extra time to execute.

IV.Block Chain Overview

The distributed monitoring process known as Blockchain is what allows Bitcoin to be generated and traded for its users.bWith no outside association oversight, this approach can strengthen the publicly available record of all Bitcoin trading activities that have previously been carried out . One advantage of blockchain technology is that once information has been verified by every hub, it cannot be changed or removed from a public ledger. This explains why Blockchain stands out in terms regarding data privacy and dependability. Additionally, blockchain technology has relationships to a variety of job types. For example, it can create a domain for global data and sophisticated contracts that are part of cloud management. The reason that the use of Blockchain approach extends in many services and applications is because of its core goal, which is data reliability.

A. METHODOLOGY

A blockchain is a collection of interconnected blocks, or an increasing amount of data that is connected by encryption. Every data block has the data to be sent, an expiration date, and the encrypted hash code of the block that came preceding it. Changing information is prohibited on the blockchain. A change to one block's data has an impact on subsequent blocks, which alters the blockchain as a whole.

Preprocessing the raw data is essential before deploying an IDS in a cloud setting. Such data sets contain a great deal of unnecessary data in addition to a wide range of assaults. As such, the most relevant aspects for the course of action must be found and separated. Following feature selection, a classifier that can distinguish between regular packets and different types of attacks will be trained using the features that were chosen. As a result, the suggested IDS in this section, which is divided into four fundamental stages: preprocessing the data, using Particle Swarm Optimising for deciding on features, correcting the discrepancy in the training data set, and putting the Distributed Tree Based One Hot Encoding (DTOHE) model into practice for producing results.

Features that the anomaly identification predicts as attacks are fed into the block chain unit as input. After that, the obtained result signature is formed, transmitted as a block in the following step, and validated. Ultimately, the signature will be dispersed among all linked nodes inside the network that is distributed. During this stage, signatures are transferred via a permissioned secure blockchain. Figure 1 depicts the broader architecture of the blockchain platform with detection of attacks.

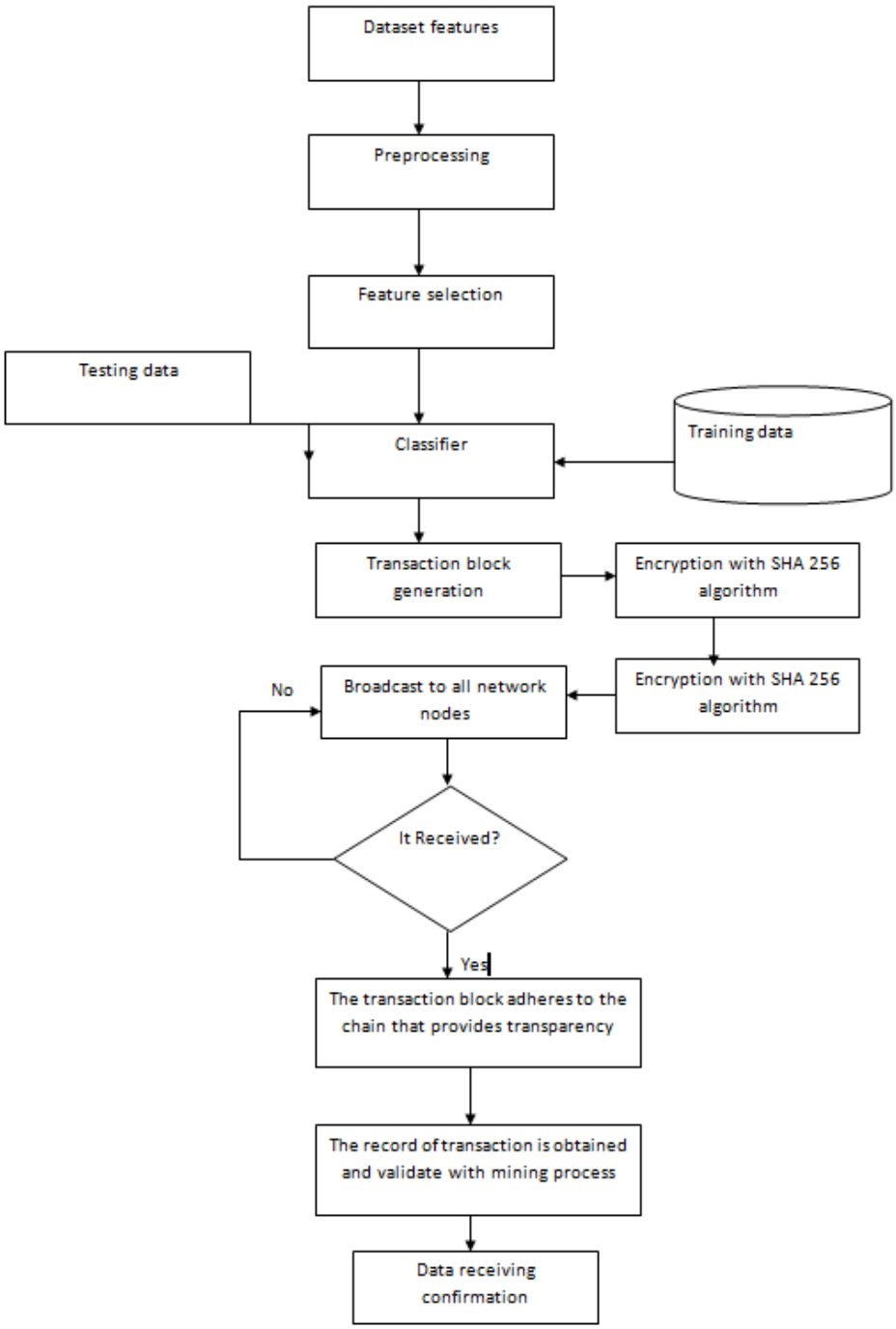

Fig 1: Architecture for intrusion detection with block chain technology

The blockchain is dispersed over a network of nodes, as seen in Figure 1. Following one of the consensus algorithms, such as proof of work (PoW), proof of stack (PoS), or proof of authority (PoA), every node in the network is connected in a distributed way.

This asymmetry technique is thought to be highly effective for safeguarding software as well as data transport via open or closed networking. It encrypts and decodes data using public and private keys. Using the data aggregation method and blockchain approach, the data is safely stored on a server. Here Proof-of-Work (PoW) for data aggregation is used. In basic terms, Proof of Work (PoW) is an incentive-dependent consensus method that requires all participants to compete for prizes in a racing variant of cryptography sector authentication. Each miner must find solutions to computationally demanding hashing challenges in order to compete in the PoW block creation. To be more precise, a viable PoW solution requires thoroughly interrogating the cryptographic algorithm for the partly created preimage from the prospective node. Finally, the candidate block's hash code must resolve specified problems in parameter h, which is the one with a predetermined bit length of zeros.

The main goal of the consensus strategy is to unite all nodes in accord, or promote mutual trust in a situation when nodes are not able to do so. A new block is then added to the blockchain system when the full transaction in the previous block has been verified. The recommended solution to blockchain-enabled data safety maintains the file on the server at the highest possible level of protection. The query parameterization rationale is used by the server's data processing logics to navigate the server while complying to appropriate cryptosecurity criteria. The degree of precision needed to preserve the data on the server has significantly increased. Information processing requires careful consideration of data alteration and avoidance in order to provide uniformity and authenticity. Data signatures and cryptography are two methods that have been used thus far to guarantee data security. Still, the confidentiality of data is guaranteed by an integral component of the blockchain methods. The unalterable nature of the blockchain makes information manipulation easier to detect. Blockchain provides shared and decentralised archived data to manage network data on the user's personal machine, preventing the chain from crashing. If a block cracking effort is made, the online database may identify them quickly, identifying differences from earlier testing and rejecting the one that doesn't match, which is a bad one. As the system is decentralised, all members of the block must confirm that the data transmitted and retained cannot be modified or erased. Due to this, the system is more reliable and well secured when compared to centralised networks.

B. Hash Function

The main component of a blockchain is a hash function. Each and every piece of data in the block is converted to hash value. The hash of the preceding square is contained in the subsequent square of a blockchain, a particular kind of hash chain. The data contained in the square cannot be added because of its unique architecture. To put it simply, hashing is the act of creating a predefined size deliverable from a supplied list containing any length. Two examples of common hash capabilities are MDA (Message Digestive Standard) and SHA (Safe Hashing Method) settings. Data transmission can be obscured and made increasingly secure by using a hash capacity. That being said, it does not account for understanding.

C. Sha-256 Algorithm

SHA-256 The National Security Agency (NSA) created the Secure Hash Algorithm, or SHA. One variant of SHA-2 (Secure Hash Algorithm 2) is the SHA-256 algorithm. A cryptographic hash function called SHA-256 has been licenced and generates a value of 256 bits in length. It is a hash algorithm, not cryptography. This cryptographic hash is only one direction. Since this algorithm's encrypted information can never be deciphered, it is extremely secure. It uses an algorithm for 256-bit block cyphers as well. The 64-character hexadecimal string is converted to 256-bit characters by SHA-256. That explains the name of the algorithm SHA-256.

Data that has been encoded is transformed into a secure version which is inaccessible unless someone else creates a key. Encrypted data can be infinitely large, frequently equal to plain data in size. In contrast, data of any size is assigned to data of a predetermined size during hashing. By means of SHA-256 hashing, for instance, a 512-bit data string would be converted to a 256-bit string.

D. Sha-256 in Security

SHA-256 is among the most secure algorithms for hashing currently in use. For this reason, blockchain makes use of it. The government of the United States requires its agencies to safeguard certain private information by employing SHA-256. SHA-256 is extremely secure because of three characteristics. 1. It is nearly impossible to reassemble the initial information contained in a hash of it. To generate the initial set of data, an attack using brute force would require 2^256 attempts. 2. It is very unusual for two messages to have the identical hash value—a situation known as a collision. In addition to The avalanche effect happens when a slight modification to the original data alters the encrypted value to the point that it is impossible to distinguish whether a fresh hashing number was produced by similar material.

Sha-256 Algorithm

Setting up W1A through W1A5

//Increase the number of 32-bit words from 16 to 64 by increasing ta from 16 to 63.

sa0=(Wia-15>>>7)⊕(Wia-15 >>>18)⊕(Wia-15 >>3)

sa1=(Wia-2>>>17)⊕(Wia-2 >>>19)⊕(Wia2 >>10)

Wta = Wia-16 + sa0 + Wia-7 + sa1

//Set this chunk's hash value to zero:

Aa = ha0 Bb = ha1 Cc = ha2 Dd = ha3 Ee = ha4 Ff = ha5 Gg = ha6 Hh = h7

The W1A - W1A5 startup is same.

//Primary loop: for ta between 0 and 63

sa0=(Aa>>>2)⊕(Aa >>>13)⊕(Aa >>>22)

mai =(Aa ∧ Bb) ∨ (Bb ∧ Cc) ∨ (Cc ∧ Aa)

t0=sa0+ mai

sa1=(Ee>>>6)⊕(Ee >>>11)⊕(Ee >>>25)

ch1 =(Ee ∧ F)f ∨ (¬Ee ∧ Gg)

taa1 = Hh + sa1 + ch1 + Kkt + Wta Hh = Gg Gg = Ff Ff = Ee Ee = Dd + taa1 Dd = Cc C c= Bb Bb = Aa Aa = ta0 + taa1

//Append this chunk's hash to the current result:

ha0 := ha0 + Aa ha1 := ha1 + Bb ha2 := ha2 + Cc ha3 := ha3 + Dd ha4 := ha4 + Ee ha5 := ha5 + Ff ha6 := ha6 + Gg ha7 := ha7 + Hh //Produce the final big-endian hash value:

digest1 = hash1 = ha0 || ha1 || ha2 || ha3 || ha4 || ha5 || ha6 || ha7

V. RESULTS AND DISCUSSION

The present investigation attempted to evaluate the performance of the suggested system, paying special emphasis to the encryption methods used by SHA-256, AES, and RSA. In order to determine how rapidly the method known as SHA-256 may protect data for different data sizes in comparison to AES and RSA, the encryption and decryption time frames. In addition, by examining the intrusion detection data, the viability and effectiveness of the blockchain-based methodology is evaluated. Also, this examined privacy settings, examined turnaround times for different data kinds on the cloud system, and confirmed that data encrypted had been transferred properly.

Table 1 Encryption time

File size (KB)	Block chain with SHA-256	AES	RSA
20	60	76	70
40	68	84	77
60	72	85	80
80	74	80	78
100	78	88	84

The comparative study of encryption durations for blockchain-SHA 256 and other current encryption methods is displayed in Table 1. When the suggested SHA-256 method is contrasted with the current cryptographic methods, the results show that using blockchain technology will shorten the encryption period. Therefore, as compared to current techniques, the suggested technique has a lower rate of encryption period.

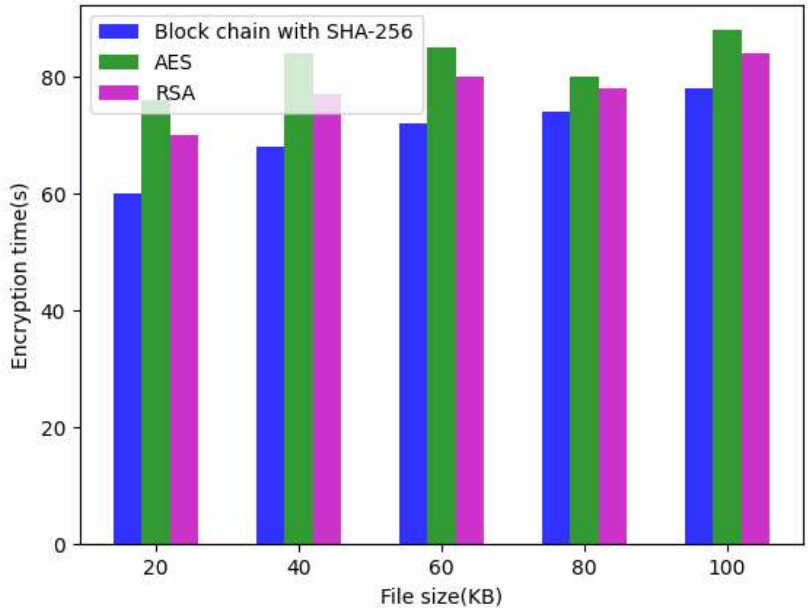

Fig 2 Encryption time comparison

The results obtained by comparing the suggested approach's encryption time to those of current cryptographic algorithms are displayed schematically in Fig. 2, and they indicate that the utilisation of blockchain will reduce the encryption duration. When compared to the current methods, the suggested method offers a shorter period of encryption duration.

Table 2: Decryption time

File size (KB)	Block chain with SHA-256	AES	RSA
20	0.85	1.05	1.5
40	0.72	0.79	1.1
60	0.69	1.77	0.8
80	0.73	0.99	0.8
100	0.81	1.02	1.1

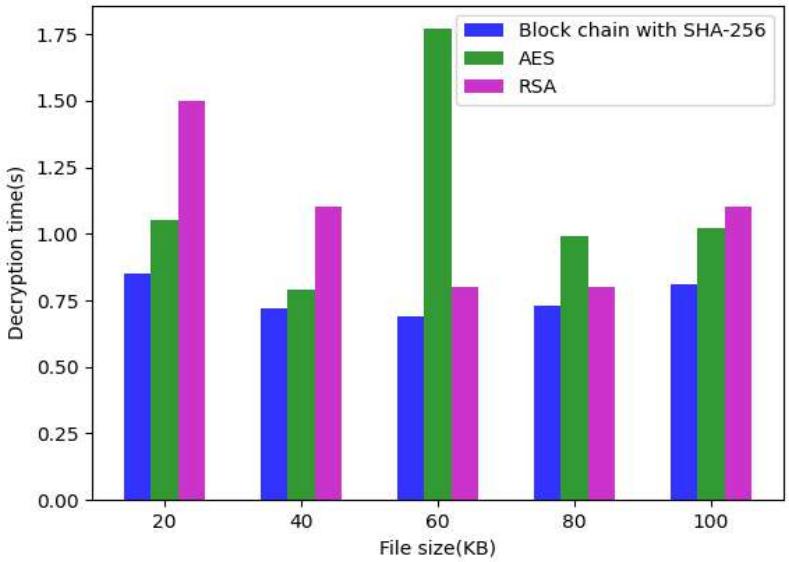

Fig 3 Decryption time comparison

Table 3 Comparative analysis of space complexity

File size (KB)	Plaintext before encryption (kb)	Ciphertext(Kb)	Plain after encryption (kb)
Block chain with SHA-256	120	128	120
AES	120	517	120
RSA	120	215	120

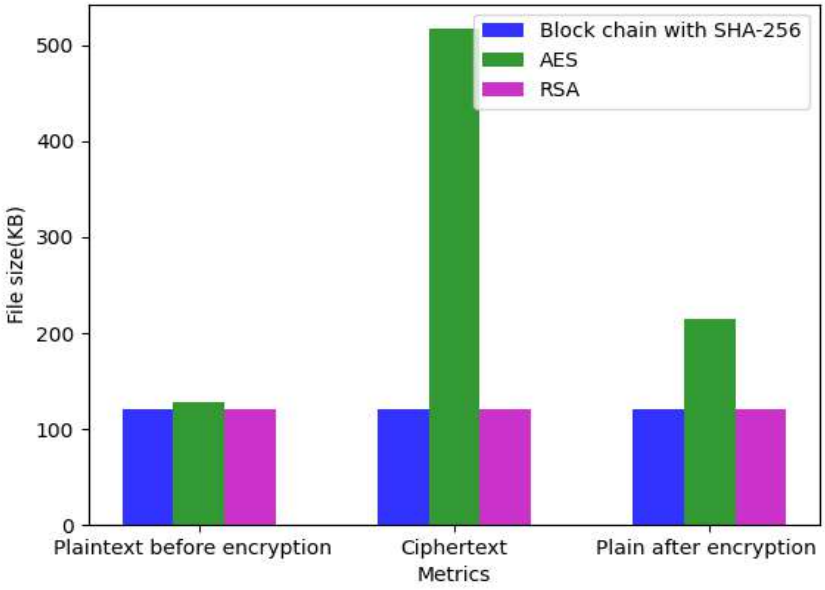

Fig 4 File size comparison

Table 4 comparative analysis of encryption algorithms

Factors	RSA	AES	SHA-256
Round(s)	1	10 - 128 bit key,12 - 192 bit key,14 - 256 bit key	64
Block Size	Variable	128 bits	512 bits
Cipher Type	Asymmetric methos	Block Cipher	Hashing algorithm
Speed	Resilient algorithm	Rapid process	Rapid process
Security	Security is low	Security is moderate	More secure

Table 3 suggests that when compared to AES and RSA, the block chain using SHA-256 has used fewer resources for storage. The relative examination of encryption techniques is displayed in Table 4. When the suggested Block chain with SHA-256 methodology is contrasted with the current cryptographic methods, Table 1's results show that using blockchain will shorten the encryption period. Therefore, as compared to current techniques, the suggested approach has a shorter period of encryption time. The findings collected expose that the recommended approach has shorter encryption duration than the present methods. Table 2 illustrates how the implementation of blockchain will result in shorter decryption duration than the current decryption techniques. As a result, in comparison to existing methods, the suggested method's duration for decryption time has dropped. Figure 3 shows that employing a block chain with the SHA 256 method reduces the amount of time needed for decryption. Figure 4 shows that the cipher text file size is significantly shorter than that of AES and RSA.

Vi.Advantages of Block Chain with Sha-256

The SHA-256 hashing method is employed by PoW blockchains to generate new blocks, validate interactions, and maintain the blockchain's security from assaults. PoW mining is enabled by the SHA-256 hash algorithm. A block hash is produced each time a new block is added to the Proof-of-Work blockchain. A miner uses the SHA-256 method to build the hash of a new block by combining data from the preceding block with a randomly generated string of integers known as the nonce.

- **Uniqueness**

Distinct hash values may always be generated from different inputs when using the SHA-256 hash algorithm. A hash value will differ greatly even with a tiny change in the input. We refer to this as the "avalanche effect."

- **Irreversibility**

Since SHA-256 hash values are extremely difficult to reverse engineer, the hash value's actual data entered cannot be extracted. By ensuring that the data is safe even in the event that the hash value is made open to everyone, this makes sharing documents convenient without being concerned about malicious actors decoding the files.

- **Deterministic**

The hash value generated by SHA-256 for a given input will never change. This characteristic makes sure that the hashing procedure remains uniform, enabling confirmation of data between distant systems.

VII.Comparison of Sha-256, Aes and Rsa

In the context of data safety, encryption algorithms such as SHA-256, AES-256, and RSA-2048 are all employed for various objectives. The Secure Hash Algorithm with 256-bit (SHA-256) is an encrypted hash algorithm that transforms an input into a string of predetermined length bytes. It fails to secure data, although it is frequently used to confirm digital signatures and data security. AES-256, often known as the Advanced Encryption Standard, is a private encryption method, requiring an identical key for both encrypting and decoding. Because of the length

of its key and the intricacy of its algorithm, it is regarded as being extremely secure and is frequently used to protect confidential information along with interactions.

A pair of public keys and private keys is used in the asymmetric encryption algorithm known as RSA-2048 (Rivest-Shamir-Adleman 2048-bit). Key swapping, digital signatures, and secure data transport are among its frequent uses. While the 2048-bit key length offers a great degree of security, it is not as fast as symmetric encryption methods such as AES.

• To sum up, RSA-2048 is an asymmetric encryption technique, AES-256 is a symmetric encryption method, and SHA-256 is a hash function. Each has a distinct function in terms of data transfer and security. A group of hashing algorithms is called SHA. In contrast, the cypher known as AES is employed for encryption purposes. A digital signature is usually accomplished through creating a hash of a few bytes and signing with a secret key. SHA algorithms (SHA-1, SHA-256, etc.) work by taking an input and generating a digest (hash).

VII.CONCLUSION

The present research offers an approach to attack identification in a decentralised block chain system. Three steps make up the offered detection system: the transaction handling phase, the intrusion identification phase, and the traffic analysis phase. In addition, to create a safe basis for the information on Blockchain, it is suggested that the intrusion detection method of the Internet of Things be used in Blockchain. The study's findings supported the authors' standards for privacy in systems that prioritise consistency and protection. In order to reduce the confidentiality of the information in a general public organization in Ecuador, a prototype algorithm was created for the research utilising flowchart methods and the blockchain. The study discovered that Blockchain technology may successfully guarantee the accuracy of the data presented to the user since, when coupled with the SHA 256 algorithm, a new digital transfer mechanism is formed that prevents accidental modifications to the data. When compared to AES and RSA algorithms, a blockchain using the SHA-256 algorithm offers superior privacy.

REFERENCES

[1] C. Badertscher, U. Maurer, D. Tschudi, and V. Zikas, ‘‘Bitcoin as a transaction ledger: A composable treatment,’’ in Advances in Cryptology— CRYPTO (Lecture Notes in Computer Science), vol. 10401. Heidelberg, Germany: Springer, 2017, pp. 324–356.

[2] I. Giechaskiel, C. J. F. Cremers, and K. B. Rasmussen, ‘‘On bitcoin security in the presence of broken cryptographic primitives,’’ in Computer Security—ESORICS (Lecture Notes in Computer Science), vol. 9879, I. G. Askoxylakis, S. Ioannidis, S. K. Katsikas, and C. A. Meadows, Eds. Heidelberg, Germany: Springer, 2016, pp. 201–222.

[3] Oliveira, Marcela T., Gabriel R. Carrara, Natalia C. Fernandes, Célio VN Albuquerque, Ricardo C. Carrano, Dianne SV Medeiros, and Diogo MF Mattos. "Towards a performance evaluation of private blockchain frameworks using a realistic workload." In 2019 22nd conference on innovation in clouds, internet and networks and workshops (ICIN), pp. 180187. IEEE, 2019.

[4] Bernabe, Jorge Bernal, Jose Luis Canovas, Jose L. Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. "Privacy-preserving solutions for blockchain: Review and challenges." IEEE Access 7 (2019): 164908-164940.

[5] Liang, Hong, Yufei Ge, Wenjiao Wang, and Lin Chen. "Collaborative intrusion detection as a service in cloud computing environment." In 2015 IEEE International Conference on Progress in Informatics and Computing (PIC), pp. 476-480. IEEE, 2015.

[6] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou and B. Zhang, "A High Performance Block-chain Platform for Intelligent Devices," 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, 2018, pp. 260-261, doi: 10.1109/HOTICN.2018.8606017.

[7] M.A. Khan, S. Abbas, A. Rehman, Y. Saeed, A. Zeb, M.I. Uddin, *et al.*A machine learning approach for blockchain-based smart home networks security,IEEE Network, 35 (3) (2020), pp. 223-229

[8] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, M. Abdallah,April. "Blockchain-based firmware update scheme tailored for autonomous vehicles", IEEE (2019), pp. 1-7

[9] A. Ruggeri, A. Celesti, M. Fazio, M. Villari ,"An Innovative Blockchain-Based Orchestrator for Osmotic Computing",Journal of Grid Computing, 20 (1) (2022), pp. 1-17

[10] R. V. Biradar, S. Avareddy and V. C. Patil, "Location Based Energy Efficient Security Mechanism in Wireless Sensor Networks using Qlearning-PSO-AES Algorithm," *2023 International Conference on Network, Multimedia and Information Technology (NMITCON)*, Bengaluru, India, 2023, pp. 1-6, doi: 10.1109/NMITCON58196.2023.10275874.

[11] A. K. Mishra, N. Tripathi, M. Vaqur and S. Sharma, "Artificial Intelligence based Security Solution for Data Encryption using AES Algorithm," *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, Erode, India, 2023, pp. 1685-1690, doi: 10.1109/ICSCDS56580.2023.10104702.

[12] S. Sankaranarayanan and G. Murugaboopathi, "Secure Intrusion Detection System in Mobile Ad Hoc Networks Using RSA Algorithm," *2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)*, Tindivanam, India, 2017, pp. 354-357, doi: 10.1109/ICRTCCM.2017.73.

[13] M. Sabarish and A. S. Arunachalam, "A Trust Secure Attacker Detection with Upgraded Deep Learning-Assistance for SDN Networks," *2023 12th International Conference on System Modeling & Advancement in Research Trends (SMART)*, Moradabad, India, 2023, pp. 121-125, doi: 10.1109/SMART59791.2023.10428532.

[14] S. Sujitha, V. Kalaivani, A. M. A. Hassan and K. Iswarya, "Protecting Data from DDOS Attack in a Cloud based Intrusion Detection System Security through Enhanced RSA Algorithm," *2023 International Conference on Sustainable Communication Networks and Application (ICSCNA)*, Theni, India, 2023, pp. 23-26, doi: 10.1109/ICSCNA58489.2023.10370229.

[15] P. K. Naik, S. Divya, M. Mohan, J. Velusamy, P. Radhakrishnan and A. S. Rajasekaran, "Protecting Data from DDOS Attack in a Cloud Based Intrusion Detection System Security through Enhanced RSA Algorithm," *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*, Greater Noida, India, 2023, pp. 966-970, doi: 10.1109/ICCSAI59793.2023.10421043.

[16] X. Zhan, H. Yuan and X. Wang, "Research on Block Chain Network Intrusion Detection System," *2019 International Conference on Computer Network, Electronic and Automation (ICCNEA)*, Xi'an, China, 2019, pp. 191-196, doi: 10.1109/ICCNEA.2019.00045.

[17] M. Kumar and A. K. Singh, "Distributed Intrusion Detection System using Blockchain and Cloud Computing Infrastructure," *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, Tirunelveli, India, 2020, pp. 248-252, doi: 10.1109/ICOEI48184.2020.9142954.

[18] W. Liang, L. Xiao, K. Zhang, M. Tang, D. He and K. -C. Li, "Data Fusion Approach for Collaborative Anomaly Intrusion Detection in Blockchain-Based Systems," in *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14741-14751, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3053842.

[19] G. Gurung, G. Bendiab, M. Shiaele and S. Shiaeles, "CIDS: Collaborative Intrusion Detection System using Blockchain Technology," *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, Greece, 2022, pp. 125-130, doi: 10.1109/CSR54599.2022.9850331.

[20] Weizhi meng, Elmar wolfgang tischhauser, qingju wang, yu wang and jinguang han,"When intrusion detection meets blockchain technology: A review", Research Challenges and Opportunities in Security and Privacy of Blockchain Technologies, IEEE access, Vol:6, 1, 2018.

[21] Chris Veness, "SHA-256 Cryptographic Hash Algorithm implemented in JavaScript |Movable Type Scripts", Movable-type.co.uk, 2020.