JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(1), MARCH, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

Performance Analysis of Data Shearing and Transaction Recording for Blockchain Technology using Cryptographic Algorithm

[1]Abdulkadir Hamidu Alkali, [1]Muhammed Zaharadeen Ahmed, [2]Abdulsalam Ya'u Gital, [2]Abubakar Umar, [3]Hajara Musa
[1]*Department of Computer Engineering, University of Maiduguri, Borno State, Nigeria,*
[2]*Department of Mathematical Sciences, Abubakar Tafawa Balewa University Bauchi, Nigeria.*
[3]*Department of Mathematical Sciences, Gombe State University, Gombe, Nigeria*

ABSTRACT
Blockchain is a data structure made up of chronologically ordered data blocks. Decentralization, integrity, data sharing, security, and other characteristics distinguish it. E-Learning platform has numerous challenges such as course credibility, credit /certification, student privacy, and course sharing. This paper uses cryptographic protocol to ensure the authenticity and integrity of the information using an Ethereum blockchain type. This means that transactions are recorded in write-only mode and contributes to transaction trust and transparency. Our methodology automates smart and secure evaluations and provide credentials using Improved Elliptic Curve Cryptography Algorithm (IECCA). It is implemented using encryption and decryption algorithm and is demonstrated using analytical and content-neutrality. We also demonstrate operation from back-end to end-users application including student and faculty members. The Level of security performance of the proposed scheme is compared with other scheme for 20MB file size. The proposed schemes achieve 83% IECCA, 78 percent DES, 76% RSA, and 70% AES respectively

ARTICLE INFO
Article History
Received: December, 2021
Received in revised form: February, 2022
Accepted: March, 2022
Published online: March, 2022

KEYWORDS
Blockchain, Cryptographic, Ethereum, and IECCA

INTRODUCTION

Security systems that can offer similar level of security for various IoT systems are in high demand, as are mechanisms that can efficiently audit and control access in a smart environment, which has resulted from the introduction of blockchain technology. The study of methods for sending messages in a secret, namely encoded information form, so that only the intended recipient can isolate the disguise and read the message is known as cryptography. The term cryptography derives from the Greek words kryptos, which means "hidden," and graphein, which means "writing" [1].

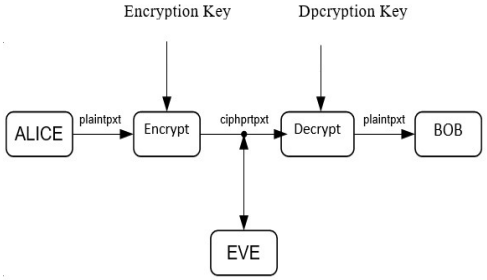

Figure 1: Basic Communication Scenario [1]

Figure 1 depicts a basic communication scenario. Two parties are considered named as Alice and Bob. They intend to communicate in a secure manner. Eve, a third party, is a potential eavesdropper. When Alice wants to send a plaintext message to Bob, she encrypts it using a predetermined method. The use of an encryption key is what

**Corresponding author:* Abdulkadir Hamidu Alkali. ahalkali@unimaid.edu.ng *Department of Computer* Engineering, University of Maiduguri, Nigeria.

keeps the message private. When Bob receives the encrypted message, known as the ciphertext, he converts it to plaintext using a decryption key.

Cryptography, on the other hand, is about more than just encrypting and decrypting messages; it is also about solving real-world problems that require information security. There are four major requirements that must be met [2]:

i. Privacy: Eve should be unable to read Alice's message to Bob. Algorithms for encryption and decryption are the primary tools.
ii. Data Integrity: Bob wants to ensure that Alice's message was not tampered with. Transmission errors, for example, could occur. An adversary could also intercept the transmission and modify it before it reaches its intended recipient. Many cryptographic primitives, such as hash functions, offer methods for ensuring data integrity in the face of malicious or unintentional adversaries.
iii. Authentication: Bob wants to ensure that the message he received was sent only by Alice. Identification schemes and password protocols are also included under this heading. In cryptography, there are two types of authentications: entity authentication and data-origin authentication. Identification is frequently used to refer to entity authentication, which can provide adequate the identity of the parties involved in a communication. Data-origin authentication is concerned with tying information about the data's origin, such as the creator and time of creation, to the data.
iv. Non-repudiation: Alice cannot deny sending the message. Non-repudiation is especially important in electronic commerce applications, where a consumer cannot deny authorization for a purchase.

LITERATURE REVIEW

Symmetric Key Algorithms

The encryption and decryption keys in symmetric key algorithms are known to both Alice and Bob. The encryption key, for example, is shared, and the decryption key can be easily calculated from it. In many cases, the encryption and decryption keys are identical. The diagram below depicts the symmetric cypher principle [1] [3].

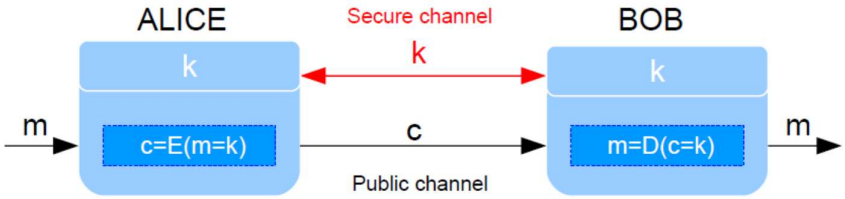

Figure 2. Principle of Symmetric Ciphers [2]

Alice uses the symmetric key k to encrypt the secret message. The ciphertext is sent to Bob over a public channel, where he can convert it back to plaintext using the symmetric key k, which must be exchanged securely before communication can begin. The system's security is based on the confidentiality of the used key. For all m 2 M; k 2 K, it has to hold that D (E (m; k); k) = m.

The proposed approach distinguishes between Block ciphers and Stream ciphers based on how the input bits are processed. Block cipher encryption algorithms take a fixed length group of bits, a block of plaintext, as input and produce a corresponding block of ciphertext, as shown in Figure 2. Stream Ciphers, as opposed to taking a block of input bits, operate on individual digits at a time, and the transformation of successive digits varies during the encryption [4]. The One-Time Pad or VERNAM Cipher is the most well-known example of a stream cipher, in which the input bits are XOR combined with the key bits. Conditions below are to be met, to ensure unbreakable cipher.

Corresponding author: Abdulkadir Hamidu Alkali. ahalkali@unimaid.edu.ng *Department of Computer* Engineering, University of Maiduguri, Nigeria.

i. Key-length = message-length,
ii. Key to be used once
iii. Key to be randomly chosen.

Cryptographic Hash Functions

A hash function used in cryptography H accepts an arbitrary length input and generates a message digest, i.e., a fingerprint of the message of a fixed length (e.g., 128 or 160 bits). Conditions are to be met to ensure hash function [5]. The message digest H(*m*) for a given message *m* can be calculated very quickly.

i. Weak Collision Resistance: Given a fingerprint y, finding *m* with H(*m*) = y is computationally impossible.
ii. Strong Collision Resistance: Finding messages *m1* and *m2* with H(*m1*) = H is computationally impossible (*m2*). This is due to the set of possible messages is larger than the set of possible hash functions. An example of messages m1 and m2 with H(*m1*) = H(*m2*) (*m2*). The final requirement states that such examples should be difficult to come by.

Blockchain Cryptography

Blockchain is a peer-to-peer (p2p) distributed database (i.e., ledger) that maintains list of continuously growing records called blocks that are linked and secured in most cases with public key cryptography [6]. Rather than adding to the centralized database in the traditional centralized system, new information is added to a block and made available to all nodes in a distributed network by blockchain technology. A hash value generated by the secure hash cryptographic algorithm-256bits (SHA256) is used to identify each block in a blockchain [7].

As shown in figure 3, the hash value of a current block header (parent) is linked and stored in the next block (child). If the content of any block changes, the hash value also changes. This change will be propagated throughout the network to invalidate that block [8]. Because blockchain technology is decentralized and distributed, it does not require an intermediary or trusted third party. Private keys are assigned to blockchain participants to digitally sign and validate transactions.

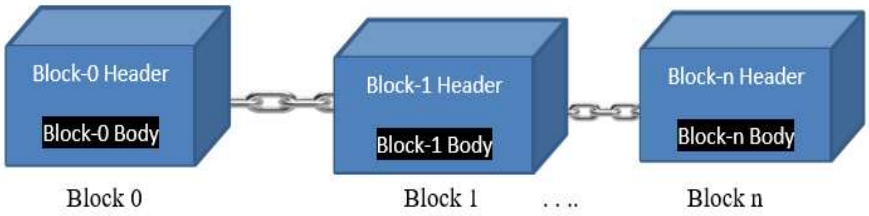

Figure 3. A Basic Blockchain [7]

The proposed work uses an ethereal blockchain to analyse the cryptographic security. Ethereum is a blockchain platform with a currency called Ether (ETH) and a programming language called Solidity. As a blockchain network, Ethereum is a decentralized public ledger for validating and recording transactions. This study used a dataset of 1000 students from 20 courses. A computer expert with a decade of experience at the e-learning center determined the courses to be included in the study using same criteria. As a result, a collaborative analysis of the dataset across multiple subjects is feasible.

The schematic representation of the proposed work is shown below (as in Figure 4).

Corresponding author: Abdulkadir Hamidu Alkali. ahalkali@unimaid.edu.ng *Department of Computer* Engineering, University of Maiduguri, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(1), MARCH, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.net

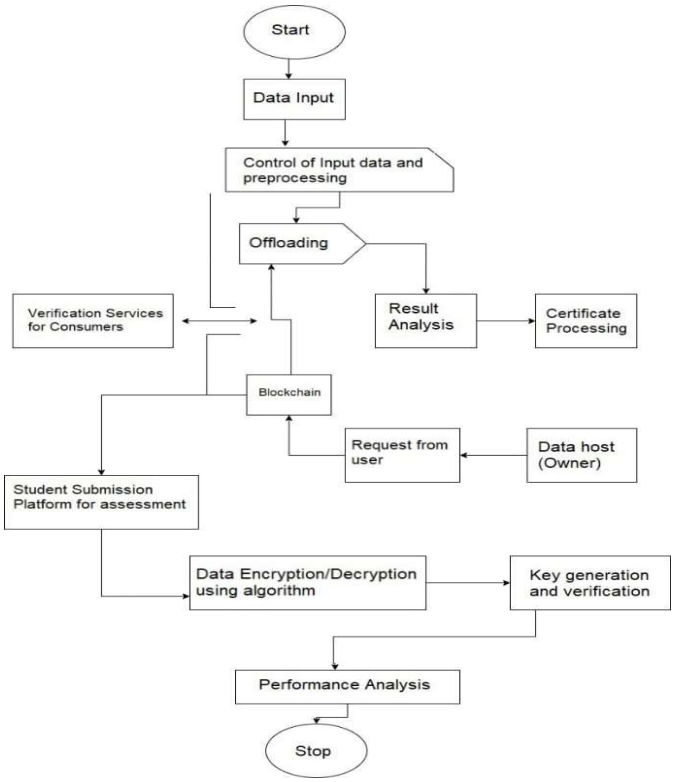

Figure 4. Schematic Representation of the Proposed Work

The proposed design enables the creation of three types of players that interact with one another via smart contracts.

i. Lecturers, teaching assistants, instructors, and other educators.
ii. Learners, which include on-campus students, online students, and others.
iii. Readers, members of the public who access or validate data, such as employers and higher education institutions.

Controlled Pre-processing

At a point, the input data has not been processed and may contain missing or repetitive packets. It has been pre-processed to remove redundant and duplicated occurrences as well as to clean up missing data. Because the dataset for the education system is large, sample size minimization techniques must be used. Because this dataset contains a large number of attributes, feature extraction tools are required to eliminate those that aren't significant. During the pre-processing stage, the dataset can be normalized. The z-score, which is expressed by Equation, is obtained in the first step of the normalization process as follows.

$$Z = [(Y - \alpha)/\omega]$$

Whereas α represents the mean of the dataset and ω denotes the standard deviation. Therefore, Z is given as follows.

$$Z = \frac{Y - \overline{Y}}{D} \quad \text{.....2}$$

Whereas Y represents the sample mean, and D represents the model's standard deviation. The random sample should follow the pattern shown below as follows.

Corresponding author: Abdulkadir Hamidu Alkali. ✉ ahalkali@unimaid.edu.ng ✉ *Department of Computer* Engineering, University of Maiduguri, Nigeria.

$$Zj = \beta 0 + \beta 1 Yj + \varepsilon j \quad \text{.....3}$$

Whereas εj denotes the errors. It is relied on the ω2. Following that, the errors must not depend on one another. Therefore, yj ∼ √ ω

$$y_j \sim \sqrt{\omega}\frac{y}{\sqrt{y^2+\omega-1}} \quad \text{.....4}$$

In equation 4, y represents a random variable. The standard deviation is then used to standardize the movement of the variables. The moment scale deviation is calculated using the expression below.

$$M = \frac{\lambda^m}{\varnothing^m} \quad \text{.....5}$$

Whereas m denotes the moment scale.

$$\lambda^m = E(Y-\alpha)^M \quad \text{.....6}$$

Whereas Y represents a random variable, and E denotes the expected value.

$$\varnothing^m = \left(\sqrt{E(Y-\alpha)^M}\right)^2 \quad \text{.....7}$$

$$y_\omega = \frac{m}{\overline{Y}} \quad \text{.....8}$$

whereas yω denotes the coefficient of the variance. After that, the feature scaling procedure will be terminated by setting all of the values to 0 or 1. This procedure is known as the unison-based normalizing approach. The normalized equation will be written as follows:

$$Y\prime = \frac{(y-y_{min})}{(y_{max}-y_{min})} \quad \text{.....9}$$

The data set can be managed once the data has been normalized, and the extent and variability of the data can be constant. This stage is primarily concerned with reducing or eliminating data latency. The normalized data can then be fed into the subsequent stages.

Data offloading and splitting

This procedure is followed because the data in the e-learning platform is massive. After preprocessing, offloading and data splitting are possible. In most prior offloading techniques, changing an information component could result in invalid data. This issue can be solved within the context of information storage by scheduling data that will be used soon. As a response, the server sends the id list of the data whose data values will be shared later, followed by the data values of the data in the id list. The id is counted down and determines when the important information will arrive at the end of the data transmission.

Algorithm 1. Encryption Process

If Ep (x, y) curve is active select relevant curve and identify all the Ep (x, y) points **then**
Return Data
Else
each intersecting point on the curve is related to an alphabet, number, or character
If An index value is assigned to alphabet, number, and character to generate index table **then**
Choose a global point P In Epusing superior-order m. (x, y)
Then a selection of a private key is done at both sender and receiver point.
Else
Assess both sender and receiver's public keys
Compute the secret key of sender and receiver
Acquire the private data by plotting it to corresponding intersection as in step 2
If Corresponding intersections generated for private data is consumed into encryption as input
Then encrypted intersections are computed using universal point P, a random integer
If Encrypted intersections and its similarity are mapped to the index value assigned in step 3
Then resultant index value is fed as an input for estimation

Corresponding author: Abdulkadir Hamidu Alkali. ahalkali@unimaid.edu.ng *Department of Computer* Engineering, University of Maiduguri, Nigeria.

Algorithm 2 is presented below as follows.

Algorithm 2. Decryption Process

Input: Index values, Prime number, x, y
Output: Private message

IF Index value generated using data encryption algorithm is used as input for decryption **then**
Return Data at the sender plane, receiver uses similar curve type Ep (x, y) and index table
Else Index value is mapped to similar character with equal encrypted IECCA points at the index table
If Receiver's secret key = (random number + universal intersection) - the encrypted points **Then**
Improved Elliptic Curve Cryptography points are mapped into characters at the index table (plaintext information).

PERFORMANCE ANALYSIS

To satisfy educational evaluations and customized curriculum, the proposed blockchain employs smart contracts on a public permissioned blockchain. It shows how this novel technology can improve a variety of key learning experiences, such as assessments, curriculum customization, and learner privacy. It was able to increase trust in educational procedures and certifications by improving transparency and authenticity while maintaining fine-grained security controls on student data.

Table 1: Simulation Parameter

S/No	Parameters	Values
1	Size	1000 x 1000m^2
2	Velocity	12, 45 m/s
3	Number of Packets	Random number between 10-15
4	Energy Aggregate	5kWh
5	Amplitude	0.0123m
6	Sampling energy	30
7	Transmission energy	80m
8	Primary & Secondary User	150, 150

Security Level using proposed Improved Elliptic Curve Cryptography Algorithm (IECCA)

The security level quantifies the strength of a cryptographic primitive, such as a cipher or hash function. Other existing strategies are compared with the proposed approach to determine the efficacy of the improved elliptic curve cryptography algorithm (IECCA). The techniques examined are Advance Encryption Algorithm (AES), Data Encryption Algorithm (DES), and Rivest Shamir Alderman (RSA), using IECCA algorithm. Level of security for 20MB file size has been 83% IECCA, 78 percent DES, 76% RSA, and 70% AES respectively. Therefore, this analysis of security level is computed for various file sizes such as 40, 60, 80, and 100 MB. As compared to different encryption approaches, the output graph presents that proposed approach (IECCA) attains high security level (as in figure 5) below.

Corresponding author: Abdulkadir Hamidu Alkali. ahalkali@unimaid.edu.ng *Department of Computer* Engineering, University of Maiduguri, Nigeria.

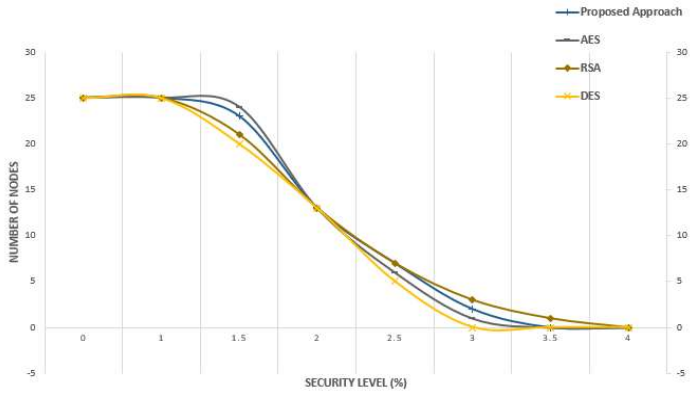

Figure 5: Proposed approach Comparison for security level (%) using different file sizes.

Execution Time

Figure 6 compares the execution times of the proposed and current methods for different file sizes, such as 20 MB, 40 MB, 60 MB, and 80 MB. The results are compared to other methods such as DES, RSA, and AES. According to the findings, the proposed approach outperforms the alternative methodologies in terms of best security performance performance.

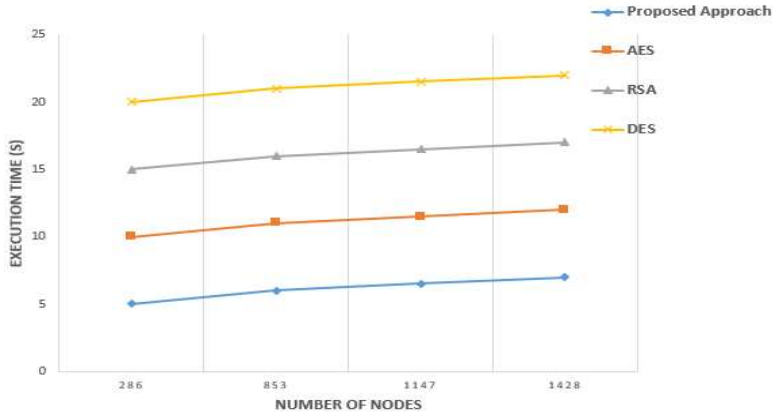

Figure 6. Proposed approach Comparison for execution time (s) for various file sizes

CONCLUSION

Blockchain technology is a novel solution for decentralized transactions and data management. It does not require the involvement of a trusted third party. It is an open and distributed ledger that allows for the verifiable recording of transactions between various parties. Blockchains have been studied in a variety of fields, including healthcare and supply chain management, but there has been little research into their potential application in intrusion detection. The proposed work implements an e-learning platform using, trust-based blockchain system to assess students' performance. This involves use of smart contracts to complete evaluations and courses by collating students' feedback as described in figure 4. The proposed work also presents how blockchain technology can enhance transparency and trust for evaluation processes and educational activities. The concept of adaptable access control guideline is highlighted on how tp achieved authorized blockchain using e-learning. The proposed work introduced an algorithm known as the improved elliptic curve cryptography algorithm (IECCA). The algorithm is presented to operate during encryption and decryption. This

Corresponding author: Abdulkadir Hamidu Alkali. ahalkali@unimaid.edu.ng *Department of Computer* Engineering, University of Maiduguri, Nigeria.

enhances the trust during evaluation on the e-learning platform. This ensures security level (%) improvement as compared to other approach DES, RSA, and AES as presented on figure 5 and 6.

REFERENCES

[1] Alshahrani, M. Y. (2021). Implementation of a blockchain system using improved elliptic curve cryptography algorithm for the performance assessment of the students in the e-learning platform. *Applied Sciences*, *12*(1), 74.

[2] Egerton, T., & Emmah, V. (2018). Comparative Analysis of Cryptographic Algorithms in Securing Data. *International Journal of Engineering Trends and Technology (IJETT)*, *58*(3), 118-122.

[3] Xu, G., Xu, S., Cao, Y., Yun, F., Cui, Y., Yu, Y., & Xiao, K. (2022). PPSEB: A Postquantum Public-Key Searchable Encryption Scheme on Blockchain for E-Healthcare Scenarios. *Security and Communication Networks*, *2022*.

[4] Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019, February). Research on the Application of Cryptography on the Blockchain. In *Journal of Physics: Conference Series* (Vol. 1168, No. 3, p. 032077). IOP Publishing.

[5] Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future generation computer systems*, *95*, 420-429.

[6] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407.

[7] Huang, S., Wang, G., Yan, Y., & Fang, X. (2020). Blockchain-based data management for digital twin of product. *Journal of Manufacturing Systems*, *54*, 361-371.

[8] Lv, Z., Qiao, L., Hossain, M. S., & Choi, B. J. (2021). Analysis of using blockchain to protect the privacy of drone big data. *IEEE Network*, *35*(1), 44-49

Corresponding author: Abdulkadir Hamidu Alkali. ahalkali@unimaid.edu.ng *Department of Computer* Engineering, University of Maiduguri, Nigeria.