International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *25 October 2023*

Enhancing Network Security Through Blockchain Technology: Challenges And Opportunities

Salwa Shakir Mahmood, Mustafa Ali Hasan, and Ayad Hasan Adhab
Ministry of Education, 10065 Al Tarbawi Collection, Baghdad, 10001, Iraq. Directorate of Education Iraq, Horror KUT, IRAQ
salwa1982m@gmail.com, m1979ah@gmail.com, ayadwasit1978@gmail.com

Abstract: The rapid proliferation of digital technologies has ushered in an era where network security is of paramount importance. Traditional security mechanisms have proven insufficient in protecting sensitive data and critical infrastructure from an ever-evolving landscape of cyber threats. Blockchain technology, originally designed to underpin cryptocurrencies like Bitcoin, has emerged as a promising solution for enhancing network security. Blockchain's core principles of decentralization, immutability, and transparency offer a unique approach to addressing vulnerabilities and mitigating risks in the digital realm. This paper examines how blockchain can enhance data integrity, authentication, and authorization processes, thereby fortifying the security posture of networks and systems.

The paper discusses real-world applications and case studies where blockchain has been successfully implemented to bolster network security, such as supply chain management, identity verification, and secure communication protocols. These examples highlight the tangible benefits and opportunities that blockchain presents for organizations seeking to safeguard their digital assets and operations. In conclusion, this abstract underscore the pivotal role that blockchain technology can play in enhancing network security. By addressing challenges head-on and capitalizing on the opportunities it offers, organizations can build resilient, transparent, and secure digital ecosystems that protect against an ever-increasing array of cyber threats. The exploration of blockchain's potential in this context is critical for shaping the future of network security in our interconnected world.

Keywords: Network Security, Blockchain Technology, Challenges, Opportunities, Cybersecurity

1. INTRODUCTION

The IoT is a paradigm that links devices with the help of the Internet network.[1] IoT is used for various intents, such as self-driving cars, healthcare, smart home, banking, wearable sensors, E-business, and surveillance systems. [2] All these devices transmit data from anywhere and anytime. During DT, the collected data faces several kinds of security challenges because the IoT is a small resource-constrained device that cannot be able to install a system or software to be highly secure. The memory usage limitation and the usage of centralized servers in IoT data collection suffer from various behaviour of intrusions. Due to the decentralized behaviour of Blockchain, it acts as a potential candidate to protect the secrecy and privacy of the IoT in a Peer-to-Peer (P2P) manner.[3]

Decentralization, P2P networking architecture, secrecy, tamper- evidence, and auditability are some of the features of Blockchain that can be useful for data sharing, transactions, and supply-chain management. [4] Because data saved on the Blockchain is highly trustworthy and easily accessible through duplication, it has piqued the interest of entire business corporations. [5] Blockchain outperforms counterpart approaches based on centralized digital ledgers by acting as a decentralized ledger that verifies and stores transaction records. [6]

The data documents in the Blockchain are stored as blocks, and the logical relationship between them is constructed as chains. If anyone performs modifications, that has been reported to the entire network using the consensus approach of Blockchain. The Blockchain does not require any intermediary entity to transmit data, leading to decentralized management. [7] This research creates a cloud data storage system based on Blockchain that employs an efficient authentication and encryption model.

2. LITERATURE REVIEW

Swan (2015) In his book titled "Blockchain: Blueprint for a New Economy," the author presents a comprehensive and in-depth analysis of the blockchain technology. This book delves into the core concepts and underlying mechanics of blockchain technology, with a specific emphasis on the technology's potential to shake up traditional economic institutions. The work done by Swan is an important and necessary resource for gaining an understanding of the conceptual foundations that drive the blockchain technology.[8]

Crosby et al. (2016) The purpose of the book named "Blockchain Technology: Beyond Bitcoin" is to provide a foundational understanding of blockchain technology. The research dives into the more technical elements of blockchain technology and highlights its potential to be used in situations

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *25 October 2023*

other than those traditionally associated with cryptocurrencies. This article lays the groundwork for comprehending the larger repercussions of blockchain technology beyond its first use by providing a platform for doing so.[9]

Iansiti and Lakhani (2017) The book "The Truth About Blockchain" gives readers an understanding of the significant and game-changing potential that blockchain technology has. The authors conduct an exhaustive study of a wide variety of applications across a variety of industries, with a special focus on the revolutionary influence that this technology has had on business processes and ecosystems. This article, which was published in the Harvard Business Review, provides useful information on the implications that blockchain technology might have in the real world.[10]

Mengelkamp et al. (2018) The purpose of this research is to evaluate the potential applications of blockchain technology within the framework of a "Blockchain-Based Smart Grid." The evaluation of sustainable local energy markets is the major focus of their research. A special emphasis is placed on the use of blockchain technology to improve the effectiveness of energy trading and consumption. This study, which focuses on practical applications, highlights the potential of blockchain technology in efficiently solving environmental challenges in real-world settings. The research was carried out by the University of Washington.[11]

Sharma et al. (2017) The author introduces "Block-VN," an architectural framework that makes use of decentralized blockchain technology and is designed for vehicle networks in smart cities. The findings of the study carried out by the authors highlight the relevance of blockchain technology in enhancing the connection and efficacy of the Internet of Things (IoT) and the infrastructure of smart cities. This research reveals that blockchain technology has the potential to improve both the safety and the performance of networks that are connected to the Internet of Things (IoT).[12]

Zheng et al. (2018) In the paper you're working on with the working title "Blockchain Challenges and Opportunities," please provide a comprehensive analysis of the themes outlined above. The study that was carried out by the writers incorporates the ideas of scalability, privacy, and consensus procedures, and as a result, it provides a holistic viewpoint on the present condition of the blockchain ecosystem. The technology known as blockchain faces a number of challenges and concerns over its safety.[13]

Trautman and Ormerod (2016) focuses on the obligations and legal ramifications that corporate directors and officers have to fulfil in order to protect the cybersecurity of their organisations. The paper discusses the standards of care required from business executives using the Yahoo data leak as a case study. It looks at how the breach prompted legal investigation and emphasizes the need for improved cybersecurity governance.[14]

Yeoh (2017) explores the problems with regulation brought on the blockchain technology. The study examines the distinctive features of blockchain and how they provide regulatory difficulties for bureaucracies and financial institutions. It addresses concerns about privacy, security, and the acceptance of blockchain transactions in law.[15]

3. PROPOSED METHODOLOGIES

This study proposes a novel mechanism to perform authentication and encryption in IoT using software-defined networks (SDN) and Blockchain. Initially, the IoT user is registered to the trusted authority (TA) and receives the key for data access using HSOA. The user is then authenticated by a TA using a user id, password and an optimal key. After successful authentication, the user encrypts their data and uploads it to the cloud. An elliptic curve integrated encryption scheme (ECIES) is used for encryption. The proposed approach performs encryption on the IoT data using ECIES. In the case of confidential data, the data is encrypted double times. Otherwise, it is encrypted only once. The user's encrypted data is stored in the cloud via the switches of SDN. The SDN uses a Blockchain mechanism to keep the user's encrypted data. In a Blockchain, a block is created for each data the user uploads.

Each block on the Blockchain includes an index of transactions, the hashing value (SHA-256) of user data, the hashing value of the previous block, and a time stamp. If any alterations to these data blocks of Blockchain have been made, they are tracked via the smart contract (SC). In the end, the user can get the evidence of data modification performed on their uploaded file with the help of an investigator as a logical graph of evidence (LGoE). The architecture of the proposed research framework is given in Figure1.

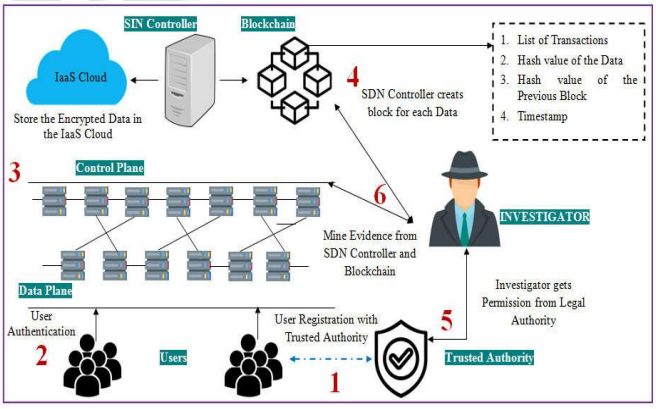

Figure1: The architecture of the proposed research framework

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *25 October 2023*

3.1. User Registration and Authentication

The first stage of the proposed model is the registration phase. In this phase, the IoT users are registered with the legal or TA in the cloud by providing their details such as name, age, date of birth, and mobile number. Once the users are registered with the TA, the TA generates a unique username, password and an optimal key using HSOA for authentication purposes and gives it to the user. The TA also stores these authentication credentials (ACs) in its cloud database to verify the user. During login, the users are asked to provide the username, password, and a random key, and the trusted authority checks the user-entered information with the information stored already in the cloud. If both of these credentials are matched, the TA allows the user as an authenticated one. Otherwise, it declined the user's permission for data access in the cloud. The key generation process using HSOA is described in the below section.

3.1.1. Key generation using HSOA

The TA verifies the IoT users using a username, password, and an optimal key. The proposed system's optimal key for authentication purposes is generated using the HSOA. HSOA is a heuristic-based optimization model motivated by the music improvisation process and can solve various optimization problems. The HSOA consists of five phases: initialization of algorithms parameters, initialization of harmony memory (HM), development of New Harmony using HM information, updating of HM, and continuation of steps 3 and 4 until the stopping criteria are met. The pseudocode of the HSOA for optimal key generation is given.

1. **Initialize** set of random keys for key generation and the HSOA's parameters (HMCR, PAR, MI, and HMS), where HMCR denotes the harmony memory considering rate, HMS- harmony memory size, PAR-pitch adjusting rate and M is the Maximum improvisation.
2. **Initialize** the harmony memory
   Generate the vectors of HM, $HM = [K_1 K_2, \ldots, K_{HMS}]$
   Identify the worst vector in HM, $K_{worst} \in [K_1 K_2, \ldots, K_{HMS}]$
3. **Improvise** the new harmony
   $K' = \beta$ // new Harmony vector
   for $(i = 1 \text{ to } n)$ do // n denotes number of random keys
   if $(M(0,1) \le HMCR)$ then // M denotes the uniform random number generator
   Begin
   $K_i' \in [K_1', K_2, \ldots, K_{HMS}]$ {**Memory Consideration**}
   if $(M(0,1) \le PCR)$ then
   $K_i' = V_{i,k \pm n}$ // $K_i' = V_{i,k}$
   end
   else
   $K_i' \in K_i$ {**Random consideration**}
   end if
   end for
4. **Update** Harmony Memory (HM)
   if $(f(K') < f(K_{worst}))$ **then** // $f(K')$ denotes the fitness of New Harmony vector and $f(K_{worst})$ denotes the fitness of worst harmony in the search space
   Include K' to the HM
   Exclude K_{worst}' from the HM
5. **Check** the stopping criteria
   while (the stopping criteria not met)
   Repeat Step 3 and 4.
6. **Return** the optimal solutions (optimal key)

3.2. Data Encryption and Storage

Once after successful authentication, the authenticated user can upload or download their data in the cloud. To provide security to the user data, here the ECIES is used by the proposed system. The proposed method classifies the user's data into sensitive and non-sensitive. Based on this sensitivity level, the ECIES encrypts the data. If the data is sensitive, it is encrypted double times using the ECIES. Otherwise, it is encrypted only once using the proposed ECIES model. ECIES is a public key cryptographic approach based on elliptic curve theory. The ECIES have a smaller key length to do encryption and offer higher security than other cryptographic algorithms. Elliptic curves used in the ECIES are the group of points which satisfy a particular mathematical equation. They are symmetrical. The encrypted data provided by the ECIES is stored in the cloud with the help of SDN switches. The algorithmic steps of ECIES to perform encryption on the user data are given.

Input: IoT user's data
Output: Encrypted data of the IoT users
// Initialization
Define the elliptic curve E as $Z^3 + ax + b$
Where a and b ⟶ Integers
//Key generation
Private Key $\langle \Pr_{key} \rangle$ ⟶ [between 0 and 1]
Public Key $\langle Pu_{key} \rangle \longrightarrow Bs * \Pr_{key}$
Bs ⟶ Base point of elliptic curve
//Encryption
1. For non-sensitive data ----Encrypted data $\langle NSE \rangle \longrightarrow (Pu_{key} + NSUD * B_s)$
2. For sensitive data Encrypted data $\langle SE \rangle \longrightarrow \langle E_1 \rangle + \langle E_2 \rangle$

Where $\langle E_1 \rangle \longrightarrow (Pu_{key} + SUD * B_s)$
$\langle E_2 \rangle \longrightarrow (Pu_{key} + E_1 * B_s)$
$\langle SUD \rangle$ ⟶ Sensitive user data
$\langle NSUD \rangle$ ⟶ Non sensitive user data
$\langle E_1 \rangle$ ⟶ Encrypted text 1
$\langle E_2 \rangle$ ⟶ Encrypted text 2 (final encrypted text for sensitive data)
//Decryption
Decrypted data $\langle Dr \rangle \longrightarrow Pu_{key} \times e - \Pr_{key}$

3.3. Blockchain for Evidence Collection

After successful encrypted data storage in the cloud, the proposed system uses an SDN controller to provide security to the cloud-stored data. The SDN controller uses the Blockchain mechanism to secure the user-encrypted data in the cloud. The Blockchain mechanism creates a list of blocks for the cloud-stored data. Each block in the Blockchain mechanism consists of the index of transactions, the hashing value of the data, the hashing value of the preceding block

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *25 October 2023*

and the timestamp. In the Blockchain mechanism, the hash value for each input data is generated utilizing the SHA-256 technique. The purpose of using the Blockchain mechanism in the proposed system is to monitor the activities performed on the cloud-stored data to provide security to the user data. The Blockchain mechanism uses smart contracts to track the data access that is performed on the user data in the cloud. Smart contracts (SCs) are equivalent to real-world contracts. SCs are fully digital, with everything being wholly distributed.

In actuality, a SC is a computer programme, which is stored within a Blockchain. The SCs in the Blockchain are distributed as well as immutable. Immutability indicates that once a contract is generated, nothing in the block can be changed again. It eliminates legal uncertainties in data access with transactions concluding a contract is processed on the Blockchain. So, any access or modifications to the cloud-stored data will be noted and reflected in the Blockchain module. The reflected details in the Blockchain contains, who accessed the original data, what type of modification has been done on the data, where the data has been modified and other such information. The detailed explanation of SDN, Blockchain in SDN and the hashing operation performed in Blockchain using SHA-256 is given in upcoming sections.

3.3.1. SDN controller

SDN is a networking zone that controls the network control plane (which handles numerous devices) as well as the data plane (forwarding plane). SDN contains various technologies, incorporating functioning segregation, automation, and virtualization of network via programmability. By separating the control and data planes, the control plane defines how the packets flow via the network's nodes. On the other hand, the data plane transfers packets from one location to another as controlled by the control plane. The data packets that reach the network switch in any networking background with SDN execution will observe the rules assembled into the switch's proprietary firmware. The centralized switch transmits these rules to the switch. Figure 2 shows some of the particular characteristics of SDN.

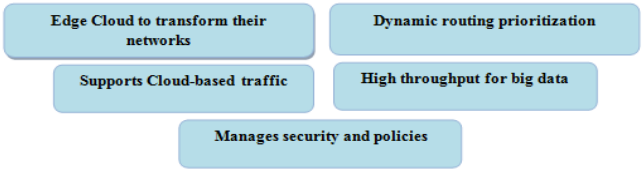

Figure 2: characteristics of SDN

The management and setting up of IoT devices are profoundly impacted by SDN. When a data packet lacks a defined route, switches in an SDN environment may submit a request for a route to a controller. This is known as dynamic routing, and it happens when switches, rather than the controller, issue route requests to routers and routing protocols. Open protocols such as OpenFlow make network control possible in SDN architectures. Instead of using closed and proprietary firmware to setup, operate, save, and optimize network resources, businesses may instead access network switches and routers at the network's edges using globally aware software control.

3.3.2. SDN controller with Blockchain

SDN controllers provide many benefits, but they also present certain security risks. It is simple for hackers to steal sensitive information from a network if they can get access to the SDN controller. Any information sent between the SDN switch and controller is vulnerable to a man in the middle attack. Therefore, in the proposed method, the Blockchain module protects IoT and SDN controllers against a variety of network assaults. Faster transactions, improved security, automated account reconciliation, fewer instances of hacking, more transparency in transactions, and varying degrees of data accessibility are only some of the benefits of using the Blockchain method in IoT data transfer. Taking these benefits of the Blockchain technology into account, the suggested concept encrypts the user's data using ECIES upon authentication. The data is then sent to a Blockchain in the cloud, where it is protected by SDN routers. The LGoE report is generated by the investigator from the Blockchain using SDN switches to verify any changes to the data. The suggested paradigm provides a more secure environment for user data in the IoT.

3.3.3. SHA-256 hashing

The Secure Hash method 2 (SHA-2) family includes many widely used cryptographic hash functions, including the SHA-256 method. It accepts data of any size and returns it formatted as 256-bit bytes. In the encryption process, the input data is changed into a secure format, which can only be decoded if the receiver has the key. It's possible that the encrypted data will be indefinitely larger than the original. In contrast, data of any size may be hashed into a uniform one. 512-bit information is shrunk to a 256-bit string size in SHA-256 hashing. A hash function produces a more secure hash result, and modifying the original hash data is difficult. SHA-256 hashing entails the following procedures:

- **Step 1:** Transform the data into binary (0’s and 1’s).
- **Step 2:** Separate the binary information into 512-bit chunks. If the block size is less than 512, add "padding" bits to make it 512 or larger.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *25 October 2023*

If the block size is more than 512, it must be divided into 512-bit chunks.

Add padding from the preceding data block if the final block is shorter than 512 bits.

- **Step 3:** Separate the data into smaller chunks, each of which should be 32 bits in size.
- **Step 4:** Compress the data using a 64-round process in which the hash values are cycled according to a certain pattern and new information is added each time.
- **Step 5:** Produce fresh hash values for the supplied data based on the result of step 4.
- **Step 6:** Create the latest iteration's SHA-256 hash value (hash digest). Figure 3 depicts the operation of SHA-256 hashing.

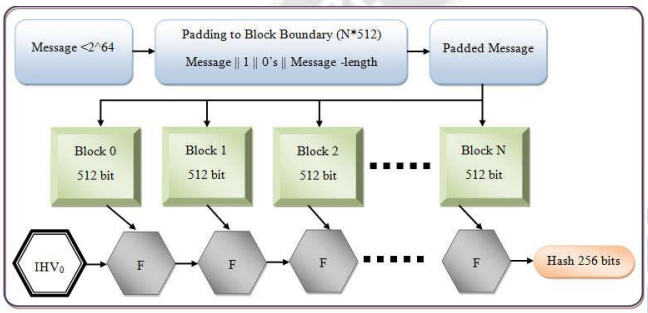

Figure 3: The working of SHA-256 hashing

3.4. Mining of Evidence Information

The cloud-based platform investigator is searching the Blockchain for relevant data. The investigator needs the TA's approval before he or she may mine the Blockchain for evidentiary information. When an investigator is given permission to access a system, they will utilised SDN controllers to mine the Blockchain for data and then create the LGoE to track down the history of modifications made to the user's data. Therefore, the suggested system offers greater security to the user data by doing all of the above in cloud data storage and keeps track of all types of misbehavior that occur in the cloud. Figure 4 is a flowchart of the suggested approach of securing the data of IoT end-users.

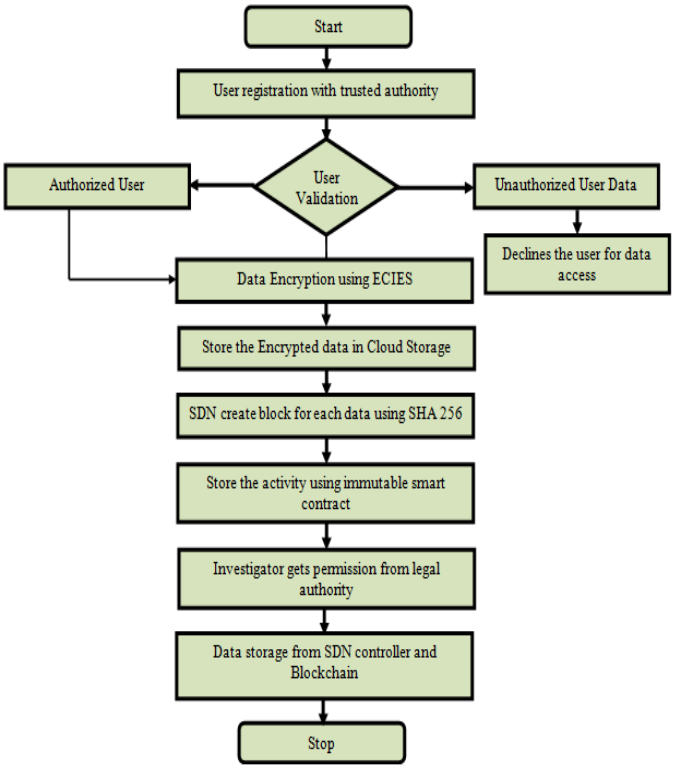

Figure 4: Data Flow Diagram

3.5. Performance Evaluation

The effectiveness of the proposed model's encryption and storage techniques for IoT data saved in the cloud is assessed in this section. Using the suggested approach, a cloud-based SDN may be built with support for 100 mobile nodes, open flow switches, Blockchain controllers, TA, and probes. After an IoT user has been verified, their submitted data is encrypted using the ECIES algorithm before being saved to the cloud. The cloud then use the Blockchain method to safeguard the data it stores.

Each user's encrypted cloud data was given a unique hash value by the Blockchain, which then stored the data in a series of blocks. The smart contracts component is also used, which detects and records any changes made to the archived information. At last, the investigator, aided by TA and SDN, performs the function of evidence mining. With TA's OK, it queries the Blockchain for a history of all SDN switch operations conducted on data stored in the cloud (LGoE). Thus, the suggested system safeguards the cloud-stored data of IoT users and, by using the Blockchain method, detects any anomalous patterns in that data. the cryptographic hash of our proposed cloud-based data storage system, as created by the Blockchain. An investigator's LGoE report for vetting users' encrypted data for wrongdoing.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *25 October 2023*

3.5.1. Performance Evaluation of ECIES

Encryption time (ETI), decryption time (DTI), computational time (CTI), and key generation time (KTI) are compared between the proposed ECIES system and current encryption models for evaluation. Advance Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Blowfish Algorithm (BFA) are the current models used for comparison. Table 3.1 displays the ETI achieved by both the proposed and the current models for 100Mb, 200Mb, 300Mb, 400Mb, and 500Mb user data files. The encryption time overhead (ETI) is the amount of time needed by an algorithm to convert plaintext into encrypted text. The proposed ECIES model requires an ETI of 3212ms to encrypt a 100Mb file, whereas the current AES, RSA, and BFA need 3543ms, 4562ms, and 6542ms, respectively.

Table 1: Assessment of Encryption Time

Encryption time (MS)					
Techniques/File Sizes (MB)	100	200	300	400	500
Proposed ECIES	3212	5213	6897	8871	10921
AES	3543	5423	7514	9162	11776
RSA	4562	6542	8762	10982	12453
BFA	6542	8712	10652	12286	14999

Table 2: Assessment of Decryption Time

		Decryption time (MS)			
Techniques/File Sizes (MB)	100	200	300	400	500
Proposed ECIES	3219	5211	6911	8882	10916
AES	3548	5412	7533	9154	11782
RSA	4561	6545	8767	10978	12453
BFA	6546	8717	10651	12289	14994

Similarly, while comparing the ETI of the encryption algorithms for various file sizes, the proposed ECIES encrypts the user's data in the least amount of time. Table 2 displays the models' DTIs. The DTI measures how long it takes an algorithm to decrypt certain data. Existing methods require more time to decrypt user data, whereas the suggested model achieves the DTI of 3219ms for 100Mb user data. Both the ETI and DTI of the models grow in tandem with the amount of the input files. While various methods can encrypt and decode user data, the suggested model can do it in much less time. Here, by using double encryption for private user information, the suggested approach achieves a marginal improvement in ETI and DTI over AES. In terms of encryption and decryption, however, it achieves a lesser value than alternatives. Figures 5 and 6 provide graphical representations of the ETI and DTI, respectively.

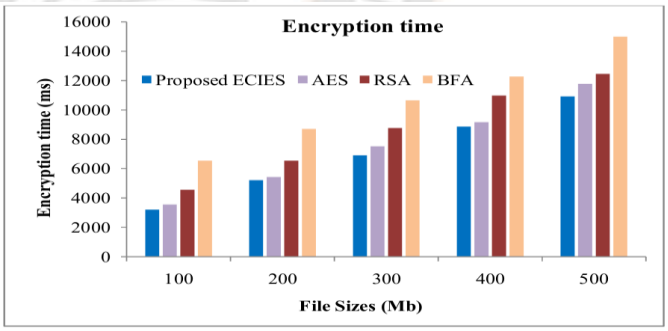

Figure 5: ETI Assessment

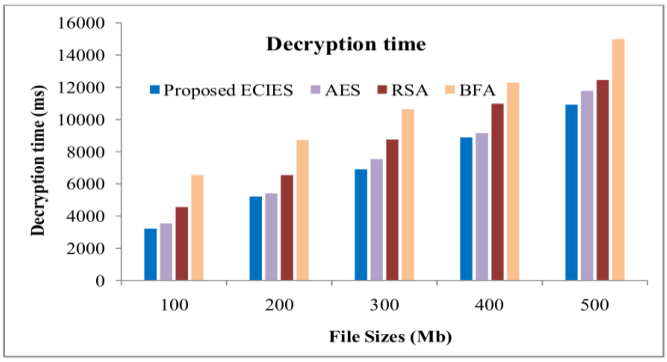

Figure 6: DTI Assessment

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *25 October 2023*

Figure 7 then shows a comparison of the encryption models using KTI. In this context, milliseconds (ms) refer to the KTI of an encryption model, which is the time required to produce keys for a cryptographic operation. Key generation for encryption and decryption in the proposed model takes 2123ms, whereas in the current AES, RSA, and BFA models, same operations take 2863ms, 3124ms, and 3876ms, respectively.

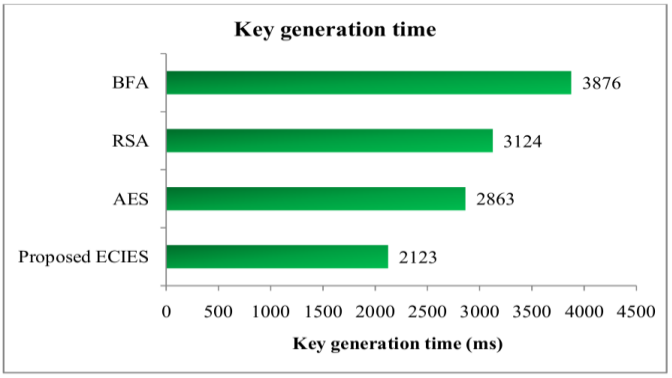

Figure 7: KTI Assessment

Since the proposed model is lightweight and uses a smaller key length for its cryptographic function, the KGT, ETI, and DTI of the proposed encryption mechanism are all reduced in comparison to existing algorithms for a key generation, as shown by the results. The next step is the evaluation-based CTI, seen in Figure 8. In this context, the CTI refers to the amount of time required to complete the whole cryptographic procedure. Changing the amount of user data (file sizes) from 100Mb to 500Mb is used to calculate the CTI. In comparison to the current methods, such as AES, RSA, and BFA, the suggested ECIES gets a CTI of 4321ms for the 100Mb data. Similarly, the ECIES has a lower CTI than AES, RSA, and BFA across the board for all file sizes tested. The analytical findings show that the proposed ECIES provides superior encryption outcomes for user data stored in the cloud.

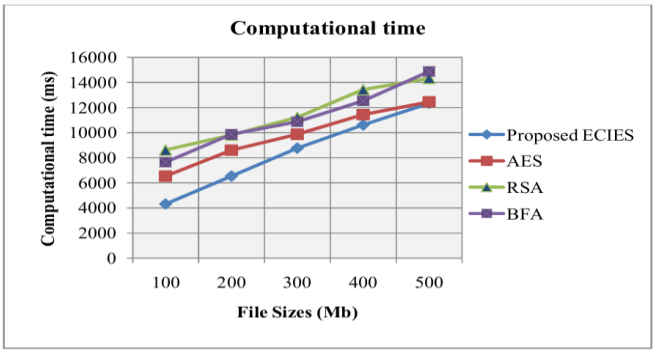

Figure 8: Evaluation of CTI

3.5.2. Performance Evaluation of Blockchain based Security Mechanism

In this part, we examine the differences between the results obtained using the current PIN-based and password-based security techniques and those obtained using the proposed security model (authentication using HSO, ECIES, and Blockchain). Data security level (SL) is used to evaluate the methods side-by-side. By shifting the file sizes between 100 and 500Mb, we can see how the models' SL changes. Table 3 summarizes the findings. To determine SL, we divide the number of unaltered bytes by the total number of bytes transferred.

Table 3: Performance Analysis regarding Security Level

		Data security level (%)	
File Sizes	Proposed	Password based	PIN based
(Mb)/Techniques	model	authentication	authentication
100	93	70	72
200	91	73	74
300	92	71	73
400	94	72	75
500	93	71	72

Table 3 shows that our suggested model achieves a better SL than the state-of-the-art models. Because the password and PIN are so simple to crack, the present methods only provide inferior protection for the user's data. The suggested methodology generates keys using the HSO and encrypts user data using the secure ECIES mechanism.

The SL of cloud-stored data has risen as a result of the increased use of security measures. In addition, the research use Blockchain technology to keep tabs on any suspicious activity involving users' data stored in the cloud. With the aid of an investigator, Blockchain's SCs generate LGoE detailing every activity linked to data changes and accesses. Therefore, the suggested model offers better protection than the current methods. Figure 9 is a graphical representation of data found in Table 3.

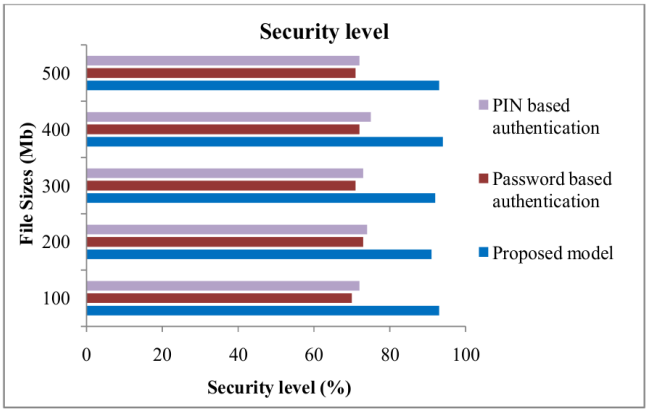

Figure 9: Evaluation of Security

3.6. Summary

Using HSOA-based optimum authentication and ECIES data encryption, this research creates a Blockchain-based data storage solution for IoT cloud users. In order to get access to the cloud storage system, the users must first authenticate with the TA. Cloud IoT user data is encrypted using ECIES after authentication, with the amount of encryption determined by the data's sensitivity. In order to prevent hackers from gaining access to users' data kept in the cloud, the Blockchain is then used to implement the encrypted data saved in the cloud. Using SDN, the detective is able to monitor all of the data modifications made to the Blockchain. Experiments are conducted to evaluate the success of the proposed secure data storage paradigm on a variety of performance metrics. When comparing ETI, DTI, CTI, and KTI, the suggested ECIES performs optimally. When compared to traditional authentication methods like passwords and PINs, the suggested Blockchain-based data storage technique offers a far greater degree of protection for cloud users' sensitive information. Since the provided solution offers improved data security for cloud IoT users, it follows that the study's findings support its adoption.

REFERENCES

1. Cachin, C. (2016). Architecture of the Hyperledger blockchain fabric. In Workshop on distributed cryptocurrencies and consensus ledgers 2016 (pp. 1-4).
2. Crosby, M., et al. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.
3. Gao, Y., & Nobuhara, H. (2017). A proof of stake sharding protocol for scalable blockchains. Proceedings of the Asia-Pacific Advanced Network, 44, 13-16.
4. Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127.
5. Kayes, A., Rahayu, W., Dillon, T., Chang, E., & Han, J. (2017). Context-aware access control with imprecise context characterization through a combined fuzzy logic and ontology-based approach. In OTM Confederated International Conferences "On the Move to Meaningful Internet Systems" (pp. 132-153). Springer.
6. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.
7. Kshetri, N. (2017). Can blockchain strengthen the Internet of Things? IT Professional, 19(4), 68-72.
8. Li, W., et al. (2017). Securing proof-of-stake blockchain protocols. Data Privacy Management, Cryptocurrencies, and Blockchain Technology, 8(1), 297-315.
9. Mengelkamp, E., et al. (2018). A blockchain-based smart grid: Towards sustainable local energy markets. Computer Science-Research and Development, 33(1), 207-214.
10. Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Block-VN: A distributed blockchain-based vehicular network architecture in a smart city. Journal of Information Processing Systems, 13(1), 184-195.
11. Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.
12. Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. (2019). A systematic literature review of blockchain cybersecurity. Digital Communications and Networks, 12(5), 1-14.
13. Trautman, L. J., & Ormerod, P. C. (2016). Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach. American University Law Review, 66(1), 1231.
14. Yeoh, P. (2017). Regulatory issues in blockchain technology. Journal of Financial Regulation and Compliance, 25(2), 196-208.
15. Zheng, Z., et al. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.