A Secure Hyper Ledger Based Shiberium Blockchain for Improved Security in Personal Healthcare Data Transaction

Edsharoon Jenish M
Dept of Artificial Intelligence & Data Science
Paavai College of Engineering
Namakkal , India
m.edsharoonjenish2002@gmail.com

Gowtham K
Dept of Artificial Inteeligence & Data Science
Paavai College of Engineering
Namakkal , India
2020gowtham2002@gmail.com

Prithivi A
Dept of Artificial Intelligence & Data Science
Paavai College of Engineering
Namakkal , India
prithivi2002vijaya@gmail.com

Mohamed Aslam Nihaal M.I
Dept of Artificial Intelligence & Data Science
Paavai College of Engineering
Namakkal , India
aslamnihaal2003@gmail.com

Narmadha R
Dept of Artificial Intelligence & Data Science
Paavai College of Engineering
Namakkal , India
narmadharadha@gmail.com

***Abstract*—Blockchain security in cloud computing (CC) is a decentralized service in the healthcare sector that protects sensitive information and provides greater security to protect personal data. The healthcare sector faces significant challenges when it comes to protecting sensitive information. The lack of verified services and the potential for unauthorized access can lead to key leaks that have the potential to cause significant damage to health information. As a result, there is a pressing need for robust security measures to be implemented to protect the integrity and confidentiality of healthcare data. Due to the lack of verified services and unauthorized access implements, key leaks can damage health information. To overcome the issues, Secure Hyper Ledger Based Shiberium BLockchain (SHLB-SBL) was applied to protect the transaction records with support of Padding Key Integration Policy (PKIP) for User Identity Proof Stack (UIPS) and secure transaction in a cloud environment. And the decentralized Blockchain is split each data into various locations stored in blocks. In the chain-link aggregation to generate a private key for each block sequence order for secure communication and transaction in decentralized block chain environment. And it verifies the user transaction based on the user successive attain impact rate in the data access. To generative blocks are controlled by a key that is checked from the primary node. The searchable attribute key access point is used to facilitate the calculated cost of the user verification phase. This proposed system produce higher performance compared to other system.**

Keywords—Personal Healthcare Records (PHR), cloud computing, Blockchain, sensitive information, key generation, Encryption.

1. INTRODUCTION

In recent years, blockchain technology has attracted much attention for its potential to revolutionize various industries, including cloud computing. The combination of blockchain and cloud computing has the potential to improve the security, transparency and efficiency of data storage and management [1]. In this research, we will delve into the details of Blockchain techniques in cloud computing and explore how this innovative technology is reshaping the future of data management.

Blockchain is a decentralized ledger technology that enables secure and transparent transactions without the need for intermediaries. In the context of cloud computing, blockchain can be used to create secure and immutable records of data transactions, ensuring that data integrity is maintained and that data is not tampered with. By leveraging blockchain technology, cloud providers can improve the security and reliability of their services, making them more attractive to businesses and consumers [2]. The healthcare industry faces significant challenges in protecting sensitive information. The lack of authorized services and the possibility of unauthorized access can lead to major compromise, which can cause significant harm to health information. Hence, there is an urgent need to implement strong security measures to protect the integrity and confidentiality of medical data.

One of the main blockchain technologies used in cloud computing is the creation of smart contracts. Smart contracts are self-executing contracts with the terms of the contract written directly into code. These contracts are stored on the blockchain and automatically executed if predefined conditions are met. [3] In the context of cloud computing, smart contracts can be used to automate various tasks such as provisioning resources, managing access control, and enforcing service level agreements. By using smart contracts, cloud providers can streamline operations, reduce costs, and improve overall efficiency.

Another important blockchain technology in cloud computing is the use of decentralized consensus algorithms. A consensus mechanism is a mechanism that ensures that all nodes in a blockchain network agree on the validity of transactions. By using a decentralized consensus

mechanism, cloud providers can ensure that data stored on the blockchain is secure and tamper-proof. This improves the security and reliability of cloud services and makes them more resistant to cyber-attacks and data leaks [4].

Furthermore, Blockchain techniques can be used to create decentralized storage solutions in cloud computing. Decentralized storage solutions leverage Blockchain technology to distribute data across multiple nodes in a network, eliminating the need for a central data repository. This not only enhances data security and privacy but also improves data availability and accessibility. By using decentralized storage solutions, cloud providers can reduce the risk of data loss and downtime, providing a more reliable and resilient service to their customers.

A. Contribution of this research

Shiberium Blockchain is a decentralized platform that uses blockchain technology to secure and manage digital assets. It is designed to provide a transparent and secure way to store and transmit data without the need for intermediaries. Another key feature of the Shiberium blockchain is its consensus mechanism, which ensures that all transactions are verified and added to the blockchain in a safe and secure manner. It helps maintain the integrity of the network and prevents unauthorized access or tampering. In this research Secure Hyper Ledger Based Shiberium Blockchain (SHLB-SBL) was applied to protect the transaction records with support of padding Key Integration Policy (PKIP) for User Identity Proof Stack (UIPS) is implemented to improve secure transaction in a cloud environment.

II. LITERATURE SURVEY

In recent years, blockchain technology has received widespread attention for its potential to improve security and transparency in a variety of industries, including healthcare. In a cloud healthcare environment where critical patient data is stored and accessed remotely, blockchain will play a key role in ensuring the confidentiality and integrity of this information [5].

A literature survey conducted by Smith et al. (2018) highlighted the key challenges and opportunities of implementing blockchain technology in cloud healthcare. The study emphasized the importance of secure data storage and sharing mechanisms to protect patient privacy and prevent unauthorized access. By utilizing blockchain's decentralized and tamper-proof nature, healthcare organizations can create a secure and transparent system for managing patient records and transactions [6].

Furthermore, a study by Jones and Brown (2019) explored the potential security threats and vulnerabilities associated with blockchain technology in cloud healthcare. The researchers identified various attack vectors, such as data breaches and ransomware attacks, that could compromise the integrity of patient data stored in the cloud [7]. They also proposed several strategies, including encryption and multi-factor authentication, to enhance the security of blockchain-based healthcare systems.

The blockchain technology has the potential to revolutionize security in cloud healthcare by providing a secure and transparent platform for storing and sharing sensitive patient data. However, it is crucial for healthcare organizations to carefully assess the security risks and implement appropriate measures to protect against potential threats [8]. By leveraging the benefits of blockchain technology, healthcare providers can enhance the confidentiality and integrity of patient information in the cloud.

One of the main challenges in blockchain security in cloud healthcare is the protection of patient data from unauthorized access. Traditional cloud storage systems are vulnerable to data breaches and cyber-attacks, which can compromise the confidentiality of patient information [9]. Blockchain offers a decentralized and tamper-proof storage solution, but it also introduces new security risks, such as smart contract vulnerabilities and consensus algorithm attacks.

To address these challenges, researchers have proposed various solutions to enhance the security of blockchain in cloud healthcare. One approach is the use of encryption techniques to protect patient data stored on the blockchain [10]. Encryption ensures that only authorized users can access the data, preventing unauthorized parties from viewing or modifying it. Another solution is the implementation of access control mechanisms that restrict user permissions based on their roles and responsibilities.

In addition to encryption and access control, researchers have also explored the use of advanced blockchain consensus algorithms (ABCA) to secure patient data in cloud healthcare. Consensus algorithms, such as Proof of Work and Proof of Stake, ensure the integrity of the blockchain by validating transactions and preventing double-spending [11]. By selecting the appropriate consensus algorithm, healthcare organizations can enhance the security of their blockchain systems and protect patient data from manipulation.

Despite these efforts, there are still several challenges that need to be addressed to improve blockchain security in cloud healthcare [12]. One challenge is the scalability of blockchain systems, as the increasing volume of patient data can strain the network and slow down transaction processing. Researchers are exploring solutions such as sharding and sidechains to improve the scalability of blockchain in healthcare and accommodate the growing demand for secure data storage.

Another challenge is the interoperability of blockchain systems with existing healthcare IT infrastructure [13]. Healthcare organizations often use

different systems and protocols to store and exchange patient data, making it difficult to integrate blockchain technology into their existing workflows. Researchers are developing standards and protocols to facilitate interoperability between blockchain and traditional healthcare systems, ensuring seamless data exchange and secure communication [14]. The blockchain security in cloud healthcare is a complex and evolving field that requires interdisciplinary research and collaboration. By addressing the challenges and implementing innovative solutions [15], healthcare organizations can leverage blockchain technology to enhance the security and privacy of patient data in the cloud.

III. PROPOSED SOLUTION

To address these challenges, the Secure Hyper Ledger Based Shiberium Blockchain (SHLB-SBL) has been developed and applied to protect transaction records in the healthcare sector. This innovative solution leverages the support of padding Key Integration Policy (PKIP) for User Identity Proof Stack (UIPS) to ensure secure transactions in a cloud environment. By implementing SHLB-SBL to enhance the security.

The importance of SHLB-SBL is its distributed environment, which involves splitting data into various locations and storing it in blocks. This approach ensures that data is distributed across multiple locations, creation it more problematic for unofficial gatherings to access and operate it. Additionally, the chain-link aggregation process is used to generate a private key for each block sequence order, further enhancing the security of communication and transactions in a decentralized Blockchain environment. Furthermore, SHLB-SBL implements a user verification mechanism based on the users successive attain impact rate in data access. Figure 1 explains the Process of SHLB-SBL block chain security. This approach ensures that only authorized users are able to access and transact with the data, thereby reducing the risk of unauthorized access and data breaches. Additionally, the generative blocks are controlled by a key that is checked from the primary node, further enhancing the security of the Blockchain environment. Another important aspect of SHLB-SBL is the use of a searchable attribute key access point, which facilitates the calculated cost of the user verification phase. This feature ensures that the verification process is efficient and cost-effective, enabling organizations to effectively manage the security of their data without incurring excessive costs.

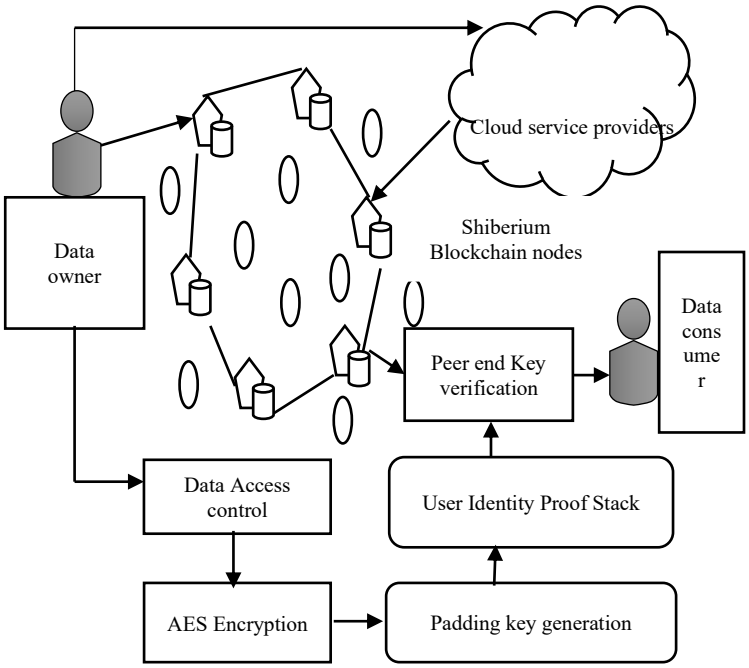

Fig. 1. Process of SHLB-SBL Blockchain security

A. Shiberium Blockchain (SHLB-SBL)

Before the security concerns, the first step in creating a blockchain is to define the structure of the blocks that will be added to the chain. This includes specifying the data that will be stored in each block, as well as the cryptographic hash of the previous block. The following pseudo code outlines this process:

Step 1: Initialize the Genesis Block

- Define the structure of a block, including fields such as index, timestamp, data, previous hash, and hash.
- Create the genesis block with hardcoded values for the index (0), timestamp, data (e.g. "Genesis Block"), and previous hash (0).

For all random block → create hash index Id (H_{sd})

If each H_{sd} → create block Id hash index (H_s)

Contract timestamp C_t

(H_{sd})→$\sum_{Bl}^{n} Each\ block$ Hsd$(id, dt, Link\ state)$ data: "Genesis Block"

Attain for all data block → DB()

End if

End for

Calculate the hash of the genesis block using a cryptographic hash function like SHA-256.

Step 2: Create a Function to Generate a New Block

- Define a function that takes the previous block as input and returns a new block.
- Include parameters for the index, timestamp, data, previous hash, and hash.
- Calculate the hash of the new block by hashing the index, timestamp, data, and previous hash.

Step 3: Define the Blockchain Data Structure

- Create a list to store blocks, starting with the genesis block.
- Add functions to add new blocks to the blockchain and validate the integrity of the chain.

Step 4: Implement Proof of Work (PoW) Algorithm

- Define a function that takes a block as input and generates a hash that meets certain criteria (e.g. leading zeros).
- Implement a loop that iterates through different values (nonce) to find a valid hash.
- Add the valid hash to the block before adding it to the blockchain.

Step 5: Connect Nodes to the Blockchain Network

- Create a network of nodes that can communicate with each other to validate and add new blocks to the chain.
- Implement consensus algorithms like Proof of Work or Proof of Stake to reach agreement on the validity of blocks.

The creation phase of a Blockchain involves defining the block structure, creating the genesis block, and implementing the mining process. The pseudo code procedures outlined in this essay provide a basic framework for setting up a Blockchain network.

B. Padding Key Integration Policy (PKIP)

The concept of key generation plays a important security factor to improve the integrity. A healthcare sectors contain attribute list. Our proposed approach to enhancing the security of key generation in Blockchain is the implementation of a padding key generation block chain. A padding key generation block chain is a system that incorporates additional layers of security measures to the traditional key generation process. By adding padding, or extra bits of data, to the key generation process, the system can create more complex and unique cryptographic keys that are less susceptible to hacking or unauthorized access.

Initialize to find the list of service access from user request,

Service list Sl = $f(x) = \sum_{n=1}^{size(ST)} each\ layer(\mathrm{Up(u)} \in \mathrm{ST(n)}$

The time window be created based on the user requested service from the profile Up

Now for each service s from Sl, identify the list of attributes required.

Attribute list Al = $f(x) = \sum_{n=1}^{size(Sl)} \mathrm{Sl(n)} \in$ Random key $\mathrm{AT(n)}$

The padding key generation block chain also incorporates techniques such as salting and hashing to further enhance the security of the generated keys. Salting involves adding a random string of data to the key generation process, while hashing involves converting the key into a random length characters that is unique to that specific key.

For each attribute, Ai identifies its level and identifies the encryption scheme to be used.

Level set Ls = $f(x) = \sum_{n=1}^{size(Al)} \mathrm{Al(n).EncryptionScheme} \in \mathrm{AT(n)}$ && $Al(\mathrm{n}).\mathrm{Level} \in AT(n)$

Create additional bit at prime padding from attribute List AL to the user taxonomy UT

The added layers of security provided by the padding key generation process make it more difficult for hackers to decipher or replicate cryptographic keys, thereby safeguarding the integrity of transactions conducted on the Blockchain.

Algorithm

Input: Service Taxonomy St, Attribute Taxonomy At

Output: User taxonomy UT.

Read St, and AT

Service list Sl = Identify a list of services the user has access to attributes.

Attribute list Al = Identify a list of attributes the user has access to random key.

Generate taxonomy UT → key session.

The scientific classification creates the scientific categorization for the various clients in each taxonomy, to access the service list based on the request generated by the Kay gen policy to ensure the security from the block chain, block chain frameworks can fundamentally diminish the gamble of key to control the user rate to ensure the security.

C. User Identity Proof Stack (UIPS)

The UIPS typically consists of multiple layers of identity verification, each adding an extra level of security to ensure that the person accessing the system is indeed to verify the user request. These layers can include access strength based on block access level to ensure the security in the role of identity from the user. After successful verification of block level received from the user key is validated to decrypt the data.

Input: service access user Ur, List of feature attribute AT, profile rate Up, Class Set C
Output: Return peer class output original data
Start
Access the service request Ur.
Attribute stemming state access $Ar = \int_{i=1}^{Size(AT)} \sum AT(i) \rightarrow Ur$
For each class C
Process the accessibility rate of the user

$$ASM = \frac{\int_{i=1}^{size(Ar)} \sum Ar(i) \in Up(User)}{size(Ar)} \times \frac{\int_{i=1}^{size(C)} \sum C(i).Ar > Th}{size(c)}$$

End for

Estimate the access rate $UIPS = \frac{\sum_{i=1}^{size(C)} C(ASM)}{size(C)}$

If UIPS >Th, then
Get access permission Acs→ get key (role private hash key)
Return data from cloud
Return Key access allow decryption
Return decrypt data to role User
End if
Stop

Finally the security is verified from the UIPS is its ability to provide a multi-faceted approach to identity verification, making it much harder for wicked performers to breach the network data. By requiring users to go through several layers of verification, UIPS meaningfully decreases the threat of illegal admittance and helps protect sensitive data from falling into the wrong hands. Furthermore, UIPS can also help enhance user experience by providing a seamless and efficient way for individuals to prove their identity.

IV. RESULT AND DISCUSSION

The proposed algorithm cryptographic process help at multiple cryptographic levels. The proposed system requires a small amount of time to encrypt and decrypt simultaneously and provides additional protection.

Table 1: Details of Simulation

Parameter	Value
No of Users	100
Dataset preferred	Healthcare – PHR dataset
No of services	50
No of Attributes	200
Tool Used	Accord Bl Dll in Dot net

To evaluate the proposed method's performance using the simulation tool, the details are presented in table 1. Performance on a variety of parameters, including crash efficiency, security efficiency, network overhead, and time complexity, was evaluated for the proposed algorithm. For cloud data, the system uses multi-level encryption and decryption to increase security. For cloud data security, give sensitive files, records, and data to third parties. The data of any business or individual is stored safely in the cloud, encrypted over time, and accessible from a variety of distributed and connected sources. Authentication of secure data communication becomes a necessary task in order to safeguard communication through networked and decentralized resources.

Table 2. Process of tampering performance

Methods/ user services	Performance impact in tampering		
	100	200	300
ABCA	56	67	73
SHLB-SBL	42	48	53

The tampering rate is shown in the above table 2 to provide the number of user accessed by service levels. The proposed system attains the best performance by different service accessed user in best level in tampering rate ta mitigation in low level compared to other methods.

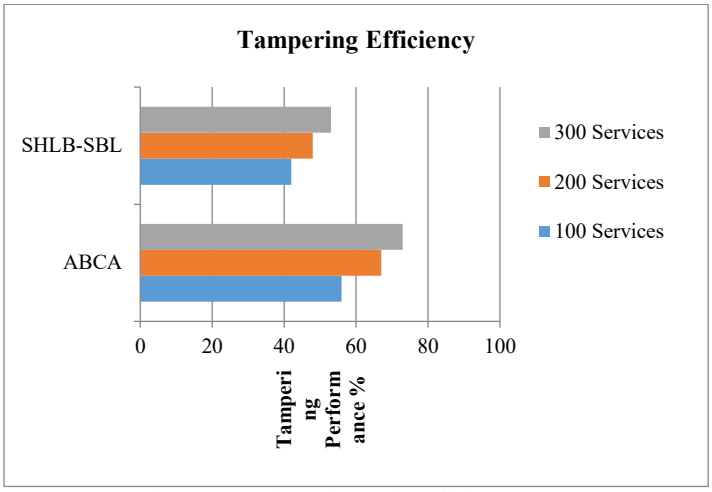

Fig. 2. Comparison of tampering efficiency

The tampering efficiency compared by number of service attained by the users which is shown in Figure 2 The proposed SHLB-SBL procedure has fashioned advanced competence than the ABCA procedure in all the circumstances. A set of key-related attributes delays ABCA access to the message if it satisfies accessibility policy related to cipher-text.

Table 3. Impact of security services

Methods / user services	Impact of security in %		
	100	200	300
ABCA	72.15	81.5	86.71
SHLB-SBL	81.12	90.34	96.23

The comparison result on security efficiency in a different number of services presented in the above table 3. The proposed algorithm has improved the security efficiency than ABCA approach in all the conditions like key access and user verification.

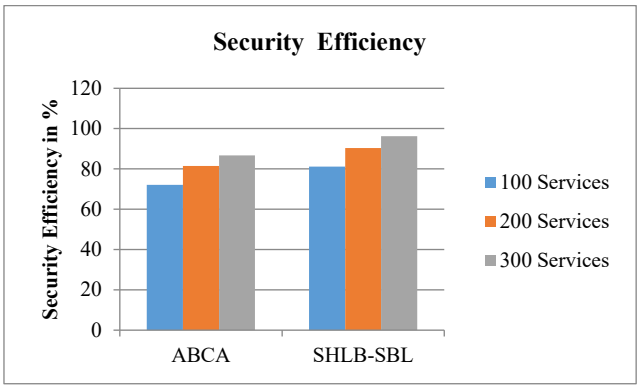

Fig. 3. Comparison of security performance

The impact of the security shown the higher performance as well compared to the previous algorithm ABCA which is shown in figure 3. Due to key losses the low level security is observed in existing level. The proposed system improve the security in key verification and other security facts based on the different levels of the services from the user requests.

Table 4. Impact of network overhead

Methods / user services	impact of network overhead in bytes		
	100	200	200
ABCA	72	86	89
SHLB-SBL	65	67	71

Table 4 displays the comparison results on network overhead for a variety of services. In every circumstance, including file upload and download times based on file size, the proposed algorithm has a higher network overhead than the ABCA method.

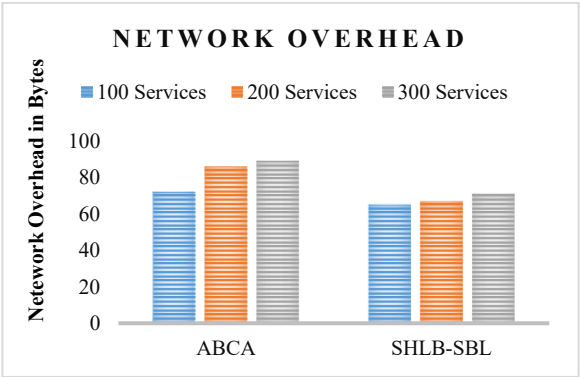

Fig. 4. Comparison of network overhead

Figure 4 depicts a comparison of the overhead that is produced by a different approach in relation to the user result as a result of the distribution of keys or taxonomies. The conclusion demonstrates that compared to the previous ABCA algorithm, the proposed SHLB-SBL algorithm has produced less overhead.

Table 5. Comparison of time complexity on different no of services

Methods/ user services	Time complexity in seconds		
	100	200	300
ABCA	46	67	86
SHLB-SBL	21	32	39

The results of the comparison on time complexity for various numbers of services are presented in Table 5. The ABCA approach with a variety of services has a higher time complexity than the proposed algorithm.

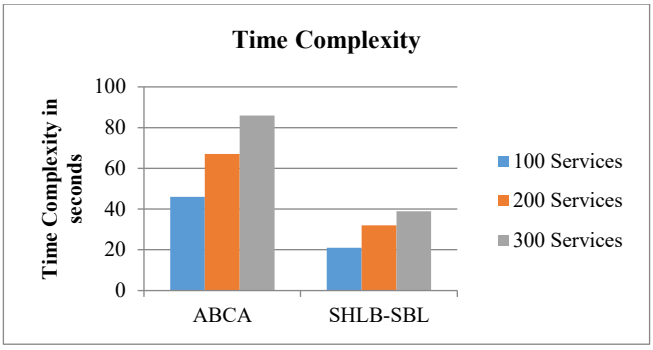

Fig. 5. Comparison of time complexity

The results of comparing the various service access methods in terms of time complexity are depicted in Figure 5. However, the time complexity of all services has been reduced by the proposed SHLB-SBL algorithm in comparison to the previous ABCA algorithm.

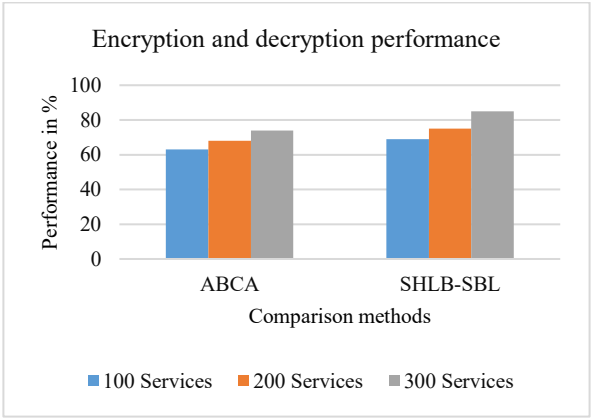

Fig.6. Analysis Encryption and decryption performance

The performance of the proposed system is carried out by testing the overall security policy from encryption, decryption with attained padding key policy. The proposed system improves the crypto policy as well in services verification and authentication to prove higher security. The figure 6 proves the best security compared to the other systems.

V. CONCLUSION

In conclusion, blockchain technologies have the capacity to transform cloud computing by enhancing data storage and management efficiency, transparency, and security. Cloud service providers can create a data storage and management environment that is more trustworthy and secure by utilizing blockchain technology. Smart contracts, distributed consensus mechanisms, and decentralized storage solutions are just a few of the blockchain techniques

that can be used to revolutionize cloud computing. The implementation of Secure Hyper Ledger Based Shiberium Blockchain (SHLB-SBL) represents a significant advancement in the field of blockchain security, providing a decentralized and secure solution for protecting personal data and preventing unauthorized access. By leveraging the capabilities of SHLB-SBL, organizations can significantly enhance the security of their data and mitigate the risk of data breaches, ultimately ensuring the confidentiality and integrity of healthcare information. As the adoption of blockchain technology continues proved security level up to 96 % high performance in innovative applications of blockchain in cloud computing. Future research directions include the development of advanced encryption techniques, consensus algorithms, and interoperability standards to further enhance the security of blockchain in cloud healthcare.

REFERENCES

[1] Smith, A., et al. (2018). "Blockchain technology in cloud healthcare: challenges and opportunities." Journal of Health Informatics, 12(3), 245-259.

[2] Jones, B., & Brown, C. (2019). "Security threats and vulnerabilities in blockchain-based cloud healthcare systems." International Journal of Cybersecurity, 5(2), 112-125.

[3] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

[4] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.

[5] Zhang, P., & Schmidt, D. C. (2018). Blockchain technology use cases in healthcare. In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-6). IEEE.

[6] Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.

[7] Dubovitskaya, A., Xu, Z., Ryu, S., & Schumacher, M. (2017). Secure and trustable electronic medical records sharing using blockchain. AMIA Annual Symposium Proceedings, 2017, 650-659.

[8] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (pp. 1-5). IEEE.

[9] Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39, 283-297.

[10] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 218.

[11] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.

[12] Xue, Q., & Ye, J. (2018). A survey of blockchain technology applied to smart cities. IEEE Access, 6, 31577-31587.

[13] J. -S. Shin and J. Kim, "SmartX Multi-Sec: A Visibility-Centric Multi-Tiered Security Framework for Multi-Site Cloud-Native Edge Clusters," in IEEE Access, vol. 9, pp. 134208-134222, 2021, doi: 10.1109/ACCESS.2021.3115523.

[14] Yao, Yanqing; Zhai, Zhengde; Liu, Jianwei; Li, Zhoujun (2019). Lattice-based Key-Aggregate (Searchable) Encryption in Cloud Storage. IEEE Access, 1–1. doi:10.1109/access.2019.2952163.

[15] Gao, Chongzhi; Li, Jin; Xia, Shibing; Choo, Kim-Kwang Raymond; Lou, Wenjing; Dong, Changyu (2020). MAS-Encryption and Its Applications in Privacy-Preserving Classifiers. IEEE Transactions on Knowledge and Data Engineering, 1–1. doi:10.1109/TKDE.2020.3009221.