International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhanced WSN Cloud Security Based on Double Linked Hash Blockchain Security using Prime Padding Rivest Cipher Key policy

R. Ramani[1*], D. Rajendra Prasad[2], CH. Mohan Sai Kumar[3],T. Karthikeyan[4], Shruti Bhargava Choubey[5], S. S. Rajasekar[6]

Submitted: 04/11/2023 **Revised**: 23/12/2023 **Accepted**: 05/01/2024

Abstract: Cloud computing and wireless sensor Network are hands on technology in recent advanced developments in healthcare sectors. Also the security is a critical concern for healthcare because of sensitive information handling is so difficult due to cryptography failures leads, key leakage problems, data breaches, integrity proofing failures and soon. The blockchain make a revolution in heath security failures to make higher end communication security. To consider this problems, propose a balck chain security based on Double Linked Hash Blocks (DLHB) using Prime Padding Rivest Cipher Key Generation policy to improve the security to protect the sensitive information. The block chain creates a Double Linked Hash Blocks (DLHB) and the collected data's are parsed to each block with hash index. The block chain creates Shuffle Structure Chain Link (SSCL) to make chain link policy to decentralized communication with Master Node Aggregation (MNA).The Blocks get encrypted with Advanced Encryption Standard (AES) and data blocks are shifted with spiral rotation. The AES model generates the block cipher key which act as communication transmission key. The Prime Padding Rivest Cipher Key Generation (PP-RCKG) policy is used to create a secret key for encrypted blocks. Then the block are circulated into chain link to make communication and key get verified by master node authentication policy to safely handover the data. The proposed system improve the security as well in security verification and validation performance, integrity proofing accuracy compared to the previous system

Keywords: *Blockchain, Cipher Key Generation, Cloud computing, Healthcare security, Prime Padding, Rivest, cloud, Shuffle Structure Chain Link, Wireless Sensor Networks*

1. Introduction

Wireless Sensor Networks (WSN) and cloud computing are revolutionizing the healthcare commerce by allowing the assortment and examination of real-time patient data. The potential applications of these technologies in healthcare are endless. From remote patient monitoring to personalized treatment plans, the possibilities are truly ground breaking With the ability to gather and analyze vast amounts of data, healthcare providers can make more informed decisions and improve patient outcomes. This innovative technology has the potential to improve patient care and outcomes, but it also raises concernsabout security and privacy. Fortunately, researchers and experts are actively working on addressing these tests. By applying strong security measures, such as encryption and authentication protocols, the healthcare industry can ensure the confidentialityand integrity of patient data [1]. The block chain is an advanced security protection in cloud communication all over the healthcare data management to provide enhanced peer end security principles. Blockchain technology has taken the world by storm, and it's not hard to see why. The security it provides is unparalleled, and the healthcare industry is no exception. The working of blockchain security in healthcare is a game-changer.

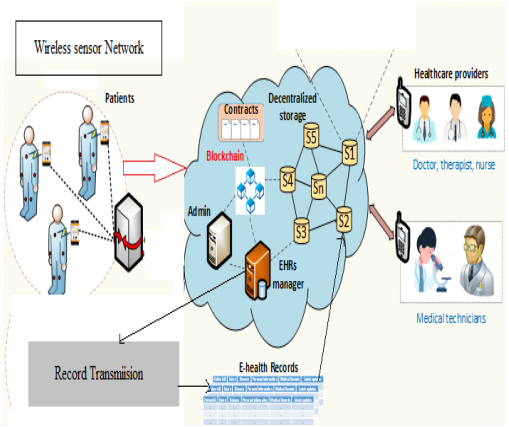

Fig 1: WSN Cloud integrated block chain security

[1]*Associate,Professor,Department of Computer Science and Engineering, P.S.R Engineering College, Sivakasi, Tamil Nadu-626140, India, Email:rramani.ananth@gmail.com*.*
[2]*Professor, Department of Electronics and Communication Engineering, St. Ann's College of Engineering & Technology, Chirala-523187. Andhra Pradesh, India. Email: rp.devathoti@gmail.com*
[3]*Assistant Professor ,Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai 600062, Tamil Nadu ,India, chmohansaikumar@veltech.edu.in.*
[4]*Assistant Professor,Department of Information Technology, University of Technology and Applied Sciences - Salalah, Sultanate of Oman, Email: karthik.rt@gmail.com.*
[5]*Dean- Innovation, Department of Electronics and Communication Engineering, Sreenidhi Institute of Science & Technology, Hyderabad-501301, Telangana, India, Shrutibhargava@sreenidhi.edu.in*
[6]*Assistant Professor,Department of Computer Science and Engineering, Bannari Amman Institute of technology, Sathyamangalam, Tamil Nadu 638401, Email:ssrajasekar80@gmail.com*

Block chain security also allows for real-time tracking of sensitive information form healthcare data. The Figure 1 describes the combination of interoperability services working in the WSN Cloud integrated block chain security. This ensures that patients receive the correct treatment and that there is no tampering with medications. It also helps to prevent counterfeit drugs from entering the market, which is a major issue in many parts of the world.Overall, the working of blockchain security in healthcare is a major step forward in protecting patient privacy and ensuring the integrity of medical data. It's exciting to see how this technology will continue to revolutionize the healthcare industry and improve patient outcomes.In the past, healthcare records have been vulnerable to breaches and cyber attacks. This puts patients' personal information at risk, and can even lead to medical identity theft. But with blockchain technology, all healthcare data is stored in a decentralized, encrypted ledger. This means that only authorized parties can access the information, and it's virtually impossible to hack. Additionally, advancements in secure cloud computing solutions are providing healthcare organizations with the security protocols they need to securely store and analyze sensitive patient information.

The potential for WSN and cloud computing in healthcare is limitless, and with the right security measures in place, the block chain security makes confidently embrace this technology to revolutionize patient care bymaintaining the sensitive information from unauthorized access [2]. The proposed systemmakes intersection of WSN(Wireless Sensor Networks), cloud computing, security, healthcare, and blockchain is an exciting and rapidly evolving field for protecting sensitive healthcare information. Thecontribution, of the proposed system creates a Double Linked Hash Blocks (DLHB) system in which collected data is parsed to each block with a hash index. The blockchain creates Shuffle Structure Chain Link (SSCL) to implement a decentralized communication policy with Master Node Aggregation (MNA). The blocks are encrypted using Advanced Encryption Standard (AES) and the data blocks are shifted with spiral rotation. The AES model generates the block cipher key, which acts as the communication transmission key. The Prime Padding Rivest Cipher Key Generation (PP-RCKG) policy is used to create a secret key for encrypted blocks. The blocks are then circulated into the chain link to facilitate communication, and the key is verified by the master node authentication policy to safely hand over the data. The WSN allows for the seamless integration of sensors and devices connected to healthcare sectors to monitor the patient information, providing real-time data on patient health and environmental conditions. The collected information’s are protected through blockchain technology, the communication ensures the security and integrity of this data, protecting patient privacy and preventing tampering.

2. Related Works

A literature review describes the integration process of WSN cloud, healthcare blockchain security is essential for understanding the current state of research in this field. This topic is of great importance as it addresses the security challenges in healthcare systems that utilize wireless sensor networks (WSN), cloud computing, and blockchain technology. By examining existing literature, researchers can gain insights into the latest advancements, identify gaps in knowledge, and propose new research directions [3]. The review will provide a comprehensive overview of the existing literature on WSN cloud healthcare blockchain security, including the challenges, solutions, and future trends. This review support valuable resource for researchers and practitioners working in this area, helping them to stay updated with the latest developments and contribute to the advancement of secure healthcare systems.

The Dual server authentication in cloud computing password authentication system. The existing system does not proper authentication protocol on the server, this system uses an Efficient Dual-Server Secret Sharing Protocol (DSSP) Based on Password Authentication for Cloud Storage Services [4]. The extended smart transportation applications sharing data andcommunication for the user authentication needs. The security system used the QueryCom designusing SHA-512 encryption to authenticate the users. The user using the method to flow communication for smart transportation [5].

Key authenticationis important for cloud users, and most of the users are using anonymous authentication schemes. Dynamic user authentication has problems with key leakage and unauthorized acess, system using Traceable Anonymous Authentication and Key Exchange Protocol is used proper authentication for users [6].The client needs a secure and efficient authentication protocol because data sharing uses proper authentication protocols for cloud servers. Most existing methodologies does not have proper authentication, so this system uses Provably Secure and Lightweight Identity-Based Authenticated Data Sharing Protocol [7].

The rapid development of wireless sensor networks and cloud computing. The new wave of technology has given to cyber security, particularly data-assisted WSNs. Prior models attains costly, so users need a low-cost and proper security system. This system uses a Lightweight Searchable public-encryption protocol [8].

Infrastructure as a Service Cloud to advanced persistent threats (APTs) is a significant are government industries to

use new technology to improve its security [8]. The security of the Iaas infrastructure technology is assured using the industry standard Cloud-Trust a Security Assessment Model [10].Data sharing is cloud computing used for multiple users using sharing and grouping to improve the efficiency of the cooperative environment and potential applications. These applications are neededfor the security level environment. The security was improved by using a Block Design-Based Key Agreement [11].

The medical cloud architecture has improved the technology based on a mobile-based cloud environment. He integrated infrastructure is needed for user authentication. User authentications are needed to improve the use of Energy-Efficient and Traceable Authentication Protocol [ETAP] [12]. The telemedical system improves the use of wireless environments for doctors and patients to meet them. The cloud server enhances the cloud security level using cipher text-policy attribute-based encryption (CP-ABE) is used to Design the Secure Authentication Protocol [13].

Mobile cloud computing refers to the cloud computing Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information Systems to improve the MCC-based multi-server authentication schemes based on the authentication of the cloud server and user[14].The cloud server remotely connects the users and shares the information remotely. The users needed for secure connection remotely and limited users using them. The security level is enhanced using the Shared Authority Privacy-PreservingAuthenticationProtocol to support user authentication privacy [15].Cloud computing is needed for efficiency, and a large number of services migrated into cloud environments. Table 1 describes the recent attentions and implementations of security principles discussed with limitations. Every user needs the authentication of the cloud users. The cloud user authentication using Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments [16].

Due to the self-organizing and random nature of sensor nodes, securing Wireless Sensor Networks (WSN) has become a more difficult task in recent years. Due to its advantages of self-organizing nature, low power consumption, and reduced cost consumption, Wireless Sensor Networks (WSNs) have grown more popular [30].

This WSN (Wireless Sensor Network) is increasingly overtaking other technologies in use in commercial and industrial applications due to considerable improvements in processor, communication, and low-power utilization of embedded computer systems [31].

Table.1 Comparison of different methodologies at the existing level

Author	***Methodology or Technique***	***Drawbacks and limitations***
B. D. Deebak., et al.,(2020)	Smart Mutual Authentication Protocol	Ley leakage , authentication failure problems
S. Roy., et al.,(2017)	Provably Secure Lightweight Remote User Authentication Scheme	Failed to protect the authentication levels
S. Chen., et al.,(2021)	Novel Strong-PUF-Based Authentication Protocols	Low level the secret key sharing
Y. Liao., et al.,(2020)	Cost-Efficient Outsourced Decryption of Attribute-Based Encryption Schemes	Failed in cryptography encryption level
S. Lin., et.,al.,(2015)	Revisiting Attribute-Based Encryption	Not high level Improvement for the encryption levels
N. H. Sultan., et al.,(2021)	Role-Based Authorized Keyword Search Scheme	Not Improved the encryption levels
J. Cui., et al.,(2023)	A Multi-Proxy Assisted Approach	Needs more the security levels
H. Cui., et al.,(2020)	Functional Encryption Using Block chain	Needs better encryption levels
H. Li., et.,al.,(2020)	Dynamic Searchable Symmetric Encryption	User needs better encryption levels
P. Gope., et.,al(2017)	Anonymous User Authentication Protocol	Needs for better authentication levels
M. A. Saleem., et.,al(2021)	Secure Three-Factor User Authentication Protocol	Needs for the authentication levels
F. Li, D. Zhong., et.,al(2012)	Practical Identity-Based Signature	Need more improvement for the security levels

3. Proposed Methodology

The proposed system improve the security levels, using double-linked hash blocks (DLHB) and collected data using a hash index based on the collected data. Then, the next SSCL-based link policy linked the chain link policy to decentralized MNA. The blocks get encrypted with AES, and data blocks are shifted with spiral rotation. The AES model generates the block cipher key, which acts as a communication transmission key. The Prime PP-RCKG policy is used to create a secret key for encrypted blocks. Then, the blocks are circulated into a chain link to facilitate communication, and the key gets verified by the master nodeauthentication policy to hand over the data safely. Performance based on security, encryption, decryption, verification and validation performance, integrity proof verification, and time complexity performances.

The working principle of WSN cloud Blockchain security is based on the wireless sensor networks (WSN), cloud computing, and blockchain technology. WSN technology is used to collect data from different sources and transmit it to the cloud for storage and processing. Cloud computing is used to provide a scalable and flexible platform for data storage and processing. Finally, Theblockchain technology is used to provide a secure and tamper-proof platform for data storage and transmission.

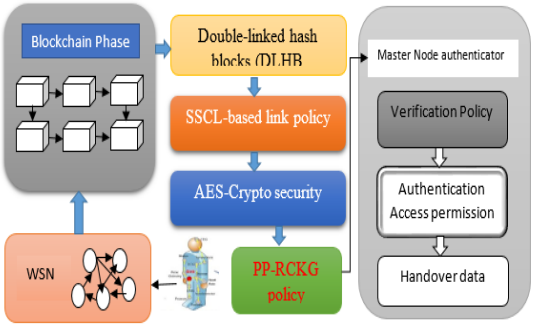

Fig 2: Proposed architecture diagram DLHB- PP-RCKG

The WSN cloud Blockchain security technology works by using a combination of encryption, authentication, and verificationtechniques to ensure that data issecure andtamper-proof. The data is encrypted before it is transmitted to the cloud, and then decrypted when it is received. Figure 2 shows the proposed architecture diagram DLHB- PP-RCKG. The Authentication techniques are used to verify the identity of the sender and receiver of the data, while verification techniques are used to ensure that the data has not been tampered with during transmission. Overall, the working principle of WSN cloud Blockchain security is an amazing technology that has the potential to revolutionize the way we secure our data. It is a powerful combination of three technologies that work together to provide a secure andreliable platform for data storage and transmission. If you are interested in learning more about this technology, I highly recommend that you do some research and explore the many benefits that it has to offer.

3.1 Double-linked hash blocks (DLHB)

The DLHB method is a new type of blockchain data structure; it is a hybrid of the traditional blockchain data structure and a linked list of the data structure. The advantage of the blockchain creates double hashing links to form scalable data structure and encrypted content block. This creates a unique identifier that is generated from a specific set of data using a mathematical algorithm. This hash id is then stored in a block on the blockchain, creating a secure and tamper-proof record of the transaction. Here w1, w2, w3, w4, w5 is numbers link blocks and the hash index id link the each block.

$$\sum w1 => \sum w2 \quad (1)$$

$$\sum \mathrm{w2} => \sum \mathrm{w3} \quad (2)$$

$$\sum \mathrm{w3} => \sum \mathrm{w4} \quad (3)$$

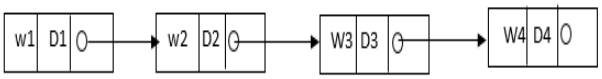

Fig.3 DLHB chain blocks

Here, w1 is linked to w2, and w2 is linked to w3, and this node is linked to w4 based on the Block d1, D2, d3 are the data blocks to be encrypt. The finally, the node w4 have stored the data and Block with hash index. Once a hash id is created and added to the blockchain, it cannot be altered or tampered with. This provides a highlevel of security and trust in the transaction process. By providing a unique identifier for each block of data, hash idsenable users to easily verify the authenticity of transactions andtrack the flow of information within the blockchain.

3.2Shuffle Structure Chain Link

The block chain create the shuffle structure of chain, the shuffling the block chain the node data would be shuffled here. Blockchain gains its name from its underlying structure. A blockchain is organized as a series of "blocks" connected in a "chain." The chain link structure refers to the way in which blocks in a blockchain are linked together in shuffled way, forming an unbreakable chain of data that cannot be altered or tampered with. Here shuffling node w1 linked to w3, and w3 linked to w2 and w4, w4 linked to w2, and w2 is linked to w1 based shuffled nodes and N is the number of nodes.

Input you're shuffling nodes $w1, w2, w3, w4, \ldots wn$ is the number of WSN nodes.

$$f(N) = \int (w1 + w2 + w3 + w4) \quad (4)$$

Here shuffling the node of equation (6),

(N)is a total number of nodes .This structure is what makes blockchains so secure, as each block in the chain contains a unique cryptographic hash that is linked to the previous block in the chain. This means that any attempt to alter or delete data in one block would require the entire chain to be altered, which is virtually impossible.

The chain link structure also ensures that data in a blockchain is transparent and easily auditable, as each block in the chain contains a complete record of all transactions that have occurred on the network

$$f(n) = \int \begin{bmatrix} w1 & w2 \\ w3 & w4 \end{bmatrix} + 1 \qquad (5)$$

Here equation (6) before shuffling the nodes

$f(x) = \iint \begin{bmatrix} w4 & w3 \\ w2 & w1 \end{bmatrix} + 1$ (6)Here equation (4,5,6) is the shuffle the nodes based on matrix format of$f(x)$.the finally shuffled node data's stored in$f(x)$. Blockchains operate by utilizing the previous hash value in the block header. This means that if one block is altered, all subsequent blocks are also affected since each block contains a hash of the previous block's header. In order to modify a block in the blockchain, an attacker would need to create a valid version of each subsequent block. The chain link structure in blockchain is a potent tool thathas the potential to revolutionize the way we store and manage data, due to its ability to offer unparalleled security.

3.3 AES key process

During this phase, the data block is encrypted using the Advanced Encryption Standard (AES) algorithm, which is the most widely used symmetric block cipher algorithm worldwide. This algorithm has a specific architecture for encrypting and decrypting sensitive data. It involves taking the original key provided by the user and expanding it into a set of round keys, which are used in the encryption and decryption process. The key expansion process involves performing a series of transformations on the original key to create a set of round keys that will be used in the subsequent rounds of the encryption process.

After the generation of the round keys, the AES working process proceeds to the initial round of the encryption process. This consists of a series of operations on the input data using the first round key. The input data is organized into a 4x4 grid of bytes, with each byte undergoing substitution and permutation operations to create a data block in spiral mode. These operations are intended to produce a complex and unintelligible representation of the input data in the output of the initial round. AES has the ability to handle key sizes such as 128, 192 and 256 bit AES on each different spiral encrypted block, and each of these ciphers has a block size of 128 bits in figure.4

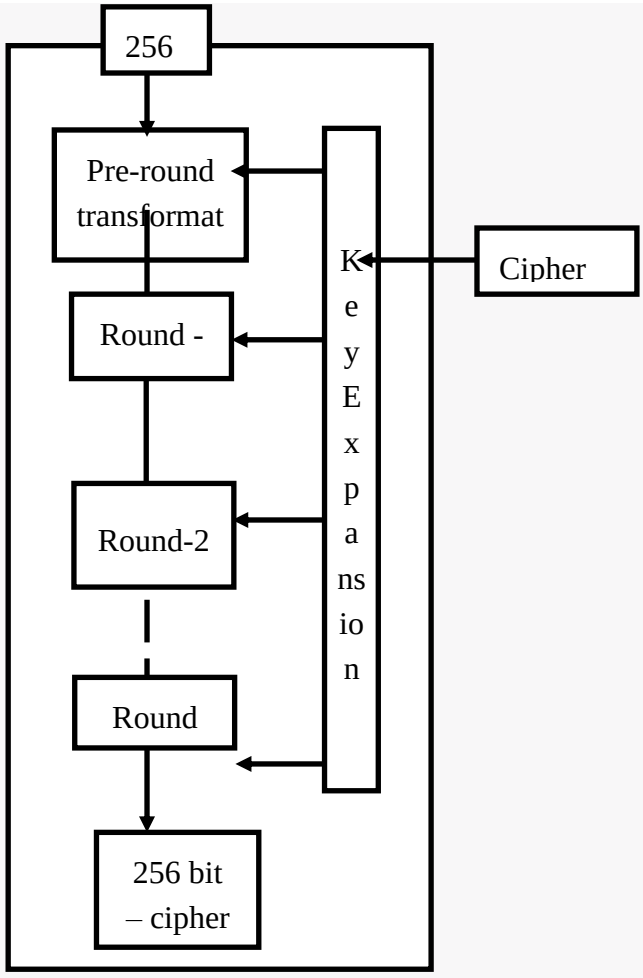

Fig 4 Advanced Encryption Standard with key work process

AES Standard Algorithm

Key Expansion (byte key [4*NK], word w [Nb*(Nr+1)]

Begin

Word temp

i=0

while (i<NK)

w[i]=word (key[4*i],key[4*i+1], key[4*i+2], key[4*i+3])

i=i+1

end while

i= NK

while (I <Nb *(Nr+1)] for each block

temp=w[i-1]

if (imodenk=0)

temp=subword(rotword(temp))

else if (NK >6 andi mod NK=4)

temp=subword (temp)

end if

w[i]=W[i-NK]xor temp At each block Piralratation

i=i+1

end while

end

Here w is the text, key parameter is generate the random key, 4*NK is the 4 round of the key process, Nb total round of the keys. the AES working process involves a Spiral creation of data blocks designed to ensure the confidentiality and integrity of sensitive information. By performing a series of substitution, permutation, and mixing operations on the input data using a set of round keys, AES is able to produce highly secure and unintelligible output data.

3.4 Prime Padding Rivest Cipher Key Generation (PP-RCKG) policy

The Prime Padding Rivest Cipher is a symmetric encryption system designed to safeguard information from unauthorized access. This paper introduces a new technique for key generation in the Prime Padding Rivest Cipher, outlining the complex process involved in encryption. The use of orthogonal matrices for generating key matrices in this cipher is explained. By employing an orthogonal matrix for key generation, the Prime Padding Rivest Cipher aims to address the issue of non-invertible matrices. This matrix-based polygraphic alternative seeks to enhance the security of encrypted data.

The setup generate the public key and master key choosing G0, binary group

$$PK = G_0, g, h = g^{\beta} + w \quad (7)$$

$$MK = (\beta, g^{\alpha}) + \text{w} \quad (8)$$

Encryption: string S plaintext encrypted message. Then the cipher text construct as

$$CT = C' = Me(g, g) \quad (9)$$

Algorithm generate the random key SK

$$SK = D = g^{(\alpha+r)}\beta \forall\ j\ \in S + \ CT \quad (10)$$

Decryption: Decryption it uses Cipher text C, Private Key SK is verify the master key policy M, and a policy attribute string S.

$$\frac{C'}{\frac{e(C,D)}{A}} = SK \quad (11$$

As such, the verification of these keys is of utmost importance in ensuring that the intended recipient is the one who is accessing the encrypted data.They can use the corresponding key to verify the authenticity of the user by aggregating MNA and ensure that it has not been compromised

3.5. Master Node Aggregation (MNA)

In block chain attention the chain-link randomization have single control based on master node policy. This contains the information about keys, block structure and shuffle keys to make validation to the user collect the information from end of the nodes. The index information $f(x)$, and all the medical data are collected and stored in$f(x)$, and here mater node M, length of the master node is q2, after S received the public. It is generate the random key r, and received the cipher text C=gm+hr.gm, it represent the multiplication of the curve points.

Chipper received by aggregation as follows:

$$C_1 = g^{m1} + h^{r1} \quad (12)$$

$$C_2 = g^{m2} + h^{r2} \quad (13)$$

Cipher text are according to receive the eqn (9) the sent chipper text is C' to received R as after verification of private key from Rivest key

$$C' = C_1 C_2 = g^{m2q1} + h^{(r_1+r_2)} \quad (14)$$

When a user receives a private Rivest key, they can verify the authenticity of the key by checking the digital signature of the certificate authority. If the signature is valid, the user can trust the key and use it for encryption and decryption.

4. Result and Discussion

This proposed system discusses the cloud security performance analysis here. Here, various functions are used in a cloud environment to analyze security. The functions are security performance, encryption performance, decryption performance, verification and validation performance, integrity proof verification performance, and time complexity performance. The following table.1 is the implementation parameters. The proposed system is compared to various algorithms. The proposed system comparison algorithms are DSSP, QUERY-COM, and ETAP. This is developed using the front end of ASP.NET with C#.NET and the back end of the proposed using MSSql-server.

Table.1 Security performance

Methods	**Performances**
DSSP	82
Query-com	85
ETAP	90
proposed	95

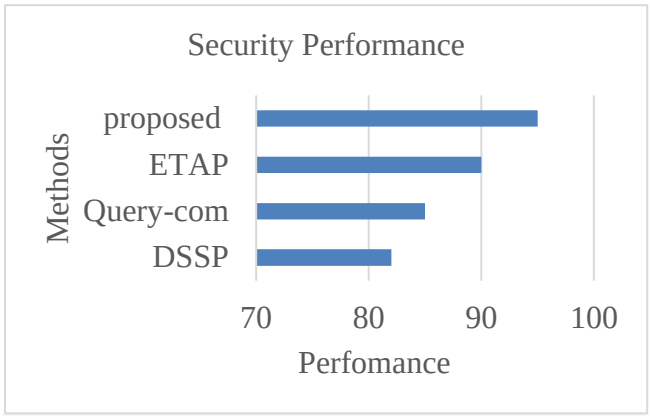

Fig .5 Security performance

Discuss the table.1 and figure.5 details about the DSSP method performance is 82%, and Query-com method security performance is 85%, and ETAP method security performance is 90%, and the proposed system performance is 95%

Table.2 Encryption performance

file size	DSSP	Query-com	ETAP	proposed
50	5	2	1	0.3
100	6	3	2	0.4
150	8	5	4	0.5
200	10	6	5	0.6

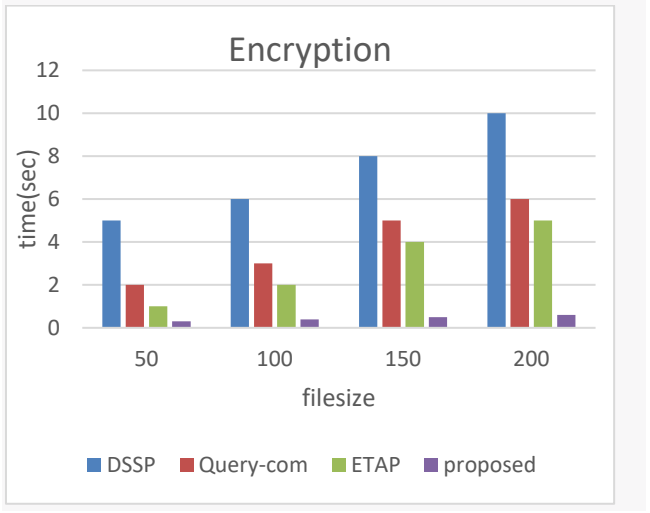

Fig. 6 Encryption performance

The table.2 and figure.6 discuss about Encryption performance for 200kbps. The performance of encryption is DSSP method is 10 m/sec, and the Query-com encryption performance is 6 m/sec, ETAP encryption performance is 5 m/sec, and the proposed system encryption performance is 0.6m/sec.

Table.3 Decryption performance

file_size	DSSP	Query-com	ETAP	proposed
50	4	3	2	0.2
100	5	4	3	0.4
150	6	5	4	0.5
200	1	7	5	0.3

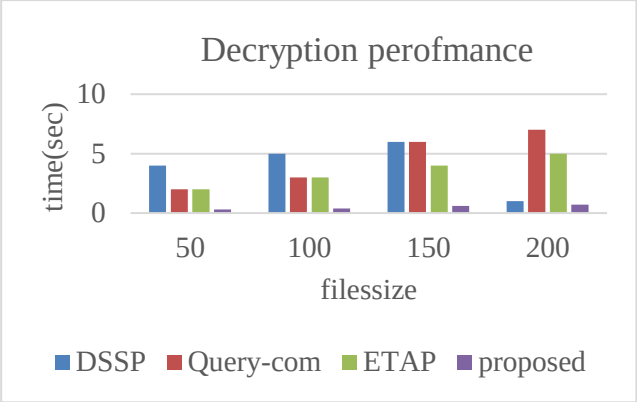

Fig. 7 Decryption predominance

The table.3 and figure.7 discuss about decryption performance for 200kbps. The performance of decryption is DSSP method is 1 m/sec, and the Query-com decryption performance is 7 m/sec, ETAP decryption performance is 5 m/sec, and the proposed system decryption performance is 0.3m/sec.

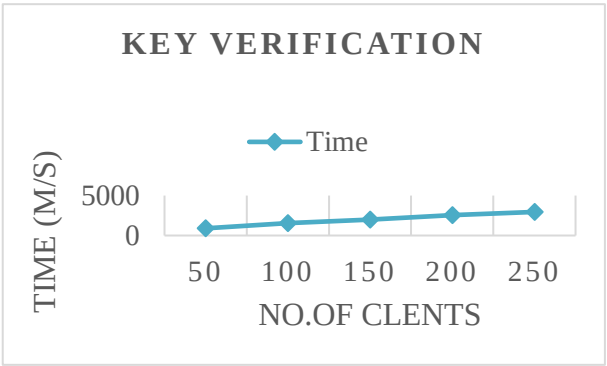

Fig. 8 verification performance

Discuss about the figure.8 key verification, The key performance for 50 user taken time is 899m/s, 100 users key verification time performance is 1550 m/s, 150 users key verification time performance is 2010 m/s, 200 users key verification time performance is 2550m/s, 250 users key verification time performance is 2950 m/s.

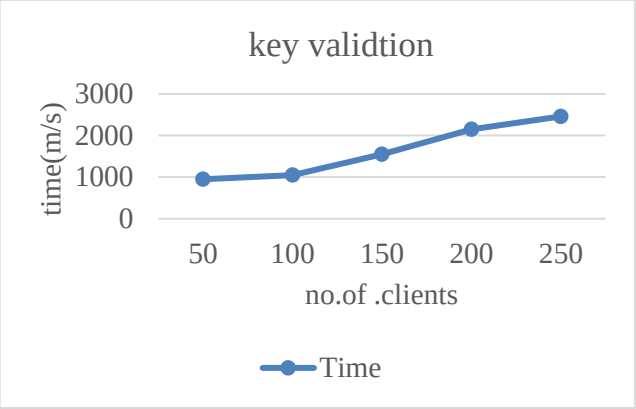

Fig 8 Validation performance

Discuss about the figure.8 key validation, The key performance for 50 user taken time is 950m/s, 100 users key validation time performance is 1050 m/s, 150 users key validation time performance is 1550 m/s, 200 users key validation time performance is 2150m/s, 2460 users key validation time performance is 2950 m/s.

Table.4 Time complexity performance

Methods	Time/sec
DSSP	**94**
Query-com	**85**
ETAP	**70**
proposed	**69**

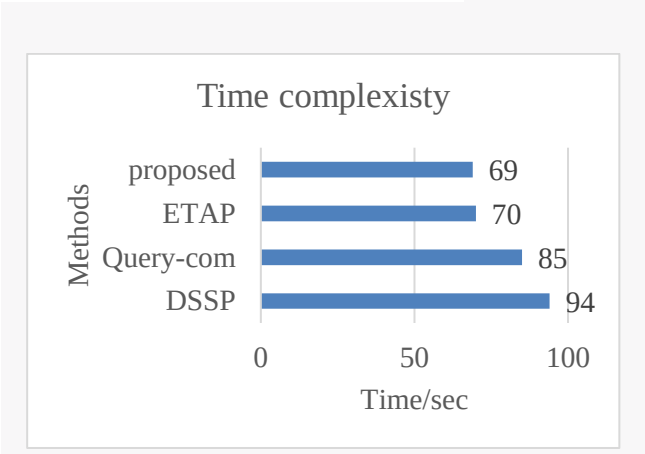

Fig 9 Time complexity performance

5. Conclusion

The proposed system based on Sensitive and non-sensitive data are separated from the information that WSNs receive and sent to the cloud server, where it is analyzed using the gynecologist dataset. The dataset in this case is the healthcare dataset. All users must get data, and any public information sent in this way needs to be sent securely. The vulnerability to hacking is the issue at hand. Key leakage, unpredictable failure, short latency, and numerous other problems are also present. The sensor medium gathers information and builds a decentralized cloud environment for logging in. Through the consensus block chain medium, the communication is carried out to maintain security. The suggested system performance is 95, the DSSP method performance is 82%, the Query-com method security performance is 85%, and the ETAP method security performance is 90%.

References

[1] M. Z. Hasan, M. Z. Hussain, Z. Mubarak, A. A. Siddiqui, A. M. Qureshi and I. Ismail, "Data security and Integrity in Cloud Computing," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, 2023, pp. 1-5, doi: 10.1109/ICONAT57137.2023.10080440.

[2] M. P. Reddy, A. M. F. Anwar, A. Sahithi and A. K. Shravani, "Data Security and Vulnerability Prevention for Cloudlet-Based Medical Data Sharing," 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2021, pp. 1477-1481, doi: 10.1109/ICECA52323.2021.9676057..

[3] M. Ali, M. -R. Sadeghi, X. Liu and A. V. Vasilakos, "Anonymous Aggregate Fine-Grained Cloud Data Verification System for Smart Health," in IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 2839-2855, 1 July-Sept. 2023, doi: 10.1109/TCC.2022.3229269.

[4] S. Zhang, X. Yong, M. Luo, D. He and K. -K. R. Choo, "DssP: Efficient Dual-Server Secret Sharing Protocol Based on Password Authentication for Cloud Storage Services," in IEEE Systems Journal, vol. 16, no. 2, pp. 2172-2182, June 2022, doi: 10.1109/JSYST.2021.3116134.

[5] T. Limbasiya and D. Das, "QueryCom: Secure Message Communication and Data Searching Protocols for Smart Transportation," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 6, pp. 5752-5764, June 2023, doi: 10.1109/TITS.2023.3249833.

[6] H. -Y. Lin, "Traceable Anonymous Authentication and Key Exchange Protocol for Privacy-Aware Cloud Environments," in IEEE Systems Journal, vol. 13, no. 2, pp. 1608-1617, June 2019, doi: 10.1109/JSYST.2018.2828022.

[7] A. Karati, R. Amin, S. H. Islam and K. -K. R. Choo, "Provably Secure and Lightweight Identity-Based Authenticated Data Sharing Protocol for Cyber-Physical Cloud Environment," in IEEE Transactions on Cloud Computing, vol. 9, no. 1, pp. 318-330, 1 Jan.-March 2021, doi: 10.1109/TCC.2018.2834405.

[8] P. Xu, S. He, W. Wang, W. Susilo and H. Jin, "Lightweight Searchable Public-Key Encryption for

Cloud-Assisted Wireless Sensor Networks," in IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3712-3723, Aug. 2018, doi: 10.1109/TII.2017.2784395.

[9] J. Luna, A. Taha, R. Trapero and N. Suri, "Quantitative Reasoning about Cloud Security Using Service Level Agreements," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 457-471, 1 July-Sept. 2017, doi: 10.1109/TCC.2015.2469659.

[10] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 523-536, 1 July-Sept. 2017, doi: 10.1109/TCC.2015.2415794.

[11] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 6, pp. 996-1010, 1 Nov.-Dec. 2019, doi: 10.1109/TDSC.2017.2725953.

[12] X. Liu and W. Ma, "ETAP: Energy-Efficient and Traceable Authentication Protocol in Mobile Medical Cloud Architecture," in IEEE Access, vol. 6, pp. 33513-33528, 2018, doi: 10.1109/ACCESS.2018.2841004.

[13] S. Son, J. Lee, M. Kim, S. Yu, A. K. Das and Y. Park, "Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain," in IEEE Access, vol. 8, pp. 192177-192191, 2020, doi: 10.1109/ACCESS.2020.3032680.

[14] A.Irshad, S. A. Chaudhry, O. A. Alomari, K. Yahya and N. Kumar, "A Novel Pairing-Free Lightweight Authentication Protocol for Mobile Cloud Computing Framework," in IEEE Systems Journal, vol. 15, no. 3, pp. 3664-3672, Sept. 2021, doi: 10.1109/JSYST.2020.2998721.

[15] H. Liu, H. Ning, Q. Xiong and L. T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 1, pp. 241-251, Jan. 2015, doi: 10.1109/TPDS.2014.2308218.

[16] W. Li, X. Li, J. Gao and H. Wang, "Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1276-1290, 1 May-June 2021, doi: 10.1109/TDSC.2019.2909890.

[17] B. D. Deebak and F. Al-Turjman, "Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of Medical Things," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 346-360, Feb. 2021, doi: 10.1109/JSAC.2020.3020599.

[18] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar and A. V. Vasilakos, "On the Design of Provably Secure Lightweight Remote User Authentication Scheme for Mobile Cloud Computing Services," in IEEE Access, vol. 5, pp. 25808-25825, 2017, doi: 10.1109/ACCESS.2017.2764913.

[19] S. Chen, B. Li, Z. Chen, Y. Zhang, C. Wang and C. Tao, "Novel Strong-PUF-Based Authentication Protocols Leveraging Shamir's Secret Sharing," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14408-14425, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3065836.

[20] Y. Liao, G. Zhang and H. Chen, "Cost-Efficient Outsourced Decryption of Attribute-Based Encryption Schemes for Both Users and Cloud Server in Green Cloud Computing," in IEEE Access, vol. 8, pp. 20862-20869, 2020, doi: 10.1109/ACCESS.2020.2969223.

[21] S. Lin, R. Zhang, H. Ma and M. Wang, "Revisiting Attribute-Based Encryption With Verifiable Outsourced Decryption," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2119-2130, Oct. 2015, doi: 10.1109/TIFS.2015.2449264.

[22] N. H. Sultan, M. Laurent and V. Varadharajan, "Securing Organization's Data: A Role-Based Authorized Keyword Search Scheme With Efficient Decryption," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 25-43, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3071304.

[23] J. Cui, B. Li, H. Zhong, Y. Xu and L. Liu, "Achieving Revocable Attribute Group-Based Encryption for Mobile Cloud Data: A Multi-Proxy Assisted Approach," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 4, pp. 2988-3001, 1 July-Aug. 2023, doi: 10.1109/TDSC.2022.3204549.

[24] H. Cui, Z. Wan, X. Wei, S. Nepal and X. Yi, "Pay as You Decrypt: Decryption Outsourcing for Functional Encryption Using Blockchain," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3227-3238, 2020, doi: 10.1109/TIFS.2020.2973864.

[25] S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang and B. Yan, "BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 7851-7867, Sept. 2020, doi: 10.1109/JIOT.2020.2993231.

[26] H. Li, Y. Yang, Y. Dai, S. Yu and Y. Xiang, "Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data," in IEEE Transactions on Cloud Computing, vol. 8, no. 2, pp. 484-494, 1 April-June 2020, doi: 10.1109/TCC.2017.2769645.

[27] P. Gope, J. Lee and T. Q. S. Quek, "Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks," in IEEE Sensors Journal, vol. 17, no. 2, pp. 498-503, 15 Jan.15, 2017, doi: 10.1109/JSEN.2016.2628413.

[28] M. A. Saleem, S. Shamshad, S. Ahmed, Z. Ghaffar and K. Mahmood, "Security Analysis on “A Secure Three-Factor User Authentication Protocol With Forward Secrecy for Wireless Medical Sensor Network Systems”," in IEEE Systems Journal, vol. 15, no. 4, pp. 5557-5559, Dec. 2021, doi: 10.1109/JSYST.2021.3073537.

[29] F. Li, D. Zhong and T. Takagi, "Practical Identity-Based Signature for Wireless Sensor Networks," in IEEE Wireless Communications Letters, vol. 1, no. 6, pp. 637-640, December 2012, doi: 10.1109/WCL.2012.091312.120488.

[30] Hemanand, D., Reddy, G. ., Babu, S. S. ., Balmuri, K. R. ., Chitra, T., & Gopalakrishnan, S. (2022). An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs). International Journal of Intelligent Systems and Applications in Engineering, 10(3), 285–293. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2167

[31] P. Satyanarayana, U. D. Yalavarthi, Y. S. S. Sriramam, M. Arun, V. G. Krishnan and S. Gopalakrishnan, "Implementation of Enhanced Energy Aware Clustering Based Routing (EEACBR)Algorithm to Improve Network Lifetime in WSN’s," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-6, doi: 10.1109/ICMNWC56175.2022.10031991.