Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

A Novel Approach for Block Chain Technology based Cyber Security in Cloud Storage Using Hash Function

Chandramohan Kanmani Pappa[1,*], Dasthegir Nasreen Banu[2], Kumar Vaishnavi[3], Susila Nagarajan[4] Manivannan Karunakaran[5], Perisetla Kandaswamy Hemalatha[6]

[1] Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Chennai-600062, Tamil Nadu, India
[2] Department of Computer Applications, B.S.Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Tamil Nadu 600048, India
[3] Department Computer Science and Engineering. Sona College of Technology, Salem, Tamil Nadu-636005, India
[4] Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore – 641008, India
[5] School of Computer Science and Engineering, Jain (Deemed -to-be) University, Bangalore, India
[6] Department of Mathematics, Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Avadi.600062, Chennai, Tamil Nadu, India

ARTICLE INFO

Article history:
Received 22 May 2023
Received in revised form 27 July 2023
Accepted 2 August 2023
Available online 5 October 2023

Keywords:
Block chain management layer; Distributed computing; Block chain cloud storage; blockchain-based Secure Information

ABSTRACT

Block chain is generic name to describe the technology used by Bitcoin and other digital currency to record and secure transaction. This technology enables a highly accessible ledger with greatly reduced risk for tampering. The dynamic immutable, data ledger makes ideal for real time monitoring of the shipment of goods. Cloud is an important of distributed storage system of networking. Cloud system need for security, storage management, minimize the cloud cost and fast storage could be improved. The security using new most development security system of block chain technology is used to improve the cloud security. The data owner to be uploads the data on web page and access the folder. The user has been accessing the data on cloud storage using encryption and decryption using block chain based cyber security system. the problem for security in cloud storage because data transmission and data sharing, the alternate for security solution using Post Quantum-proof cryptography algorithm is used to improve the encryption and decryption process and more tight security for block chain technology for the cloud system. The SHA-3 512 Hash function algorithm automatically generate the key for data security enhancements of cloud networks. Post Quantum-proof cryptography algorithm has been improved the encryption Performance and reduced the power consumption, and increase the Latency performance, and boost up the security performances. Finally Post Quantum-proof cryptography algorithm for well support for security system of the cloud networks. Even some passwords, which are often cited as the weakest link in cyber security, may not be necessary.

1. Introduction

Subsequently, a ton of organizations have moved to distributed storage, which offers extraordinary capacity, stacking, and circulation abilities. The essential issues they experience

* *Corresponding author.*
E-mail address: kanmanipappa.phd@gmail.com

https://doi.org/10.37934/araset.32.3.178189

Distributed computing ought to keep up with information trustworthiness and mystery to help with information security. By and by, there are very few copyright and information security chances. The way that anybody can see the information when it is communicated to an outside climate is the major issue. Data the elevated degree of safety vital for legitimate information security and protection isn't given by cloud specialist organizations. As of now there are not many devices and strategies for safeguarding information put away in the cloud. In this manner, propose involving Blockchain as a confided in climate to increment distributed storage security and shield against exploit assaults.

Blockchain is a decentralized framework which can't be changed. Electronic record of a P2P relationship for the record of tasks. The vault for all time stores esteem based information between centers in the relationship of a coordinated chain of hashed cryptographic blocks and is imparted to all taking part centers. The saying "blockchain" alludes to a chain of related and connected blocks of affirmed and upheld trades that reaches out from one finish to the genuine coordination community. Thusly, the block chain acts like a single information source, with all clients in the association seeing the trades they support [1].

Blockchain is an innovation that permits all clients to make a record with all the exchange information and change their records to keep their legitimacy when an exchange is made. Since the improvement of the web and cryptographic innovation, all gatherings can now autonomously affirm the trustworthiness of the exchange, dispensing with the weak link that could have come about because of depending entirely on an authority outsider match. This sort of disseminated record exists. To lay out long-lasting, invulnerable capacity of value-based information.

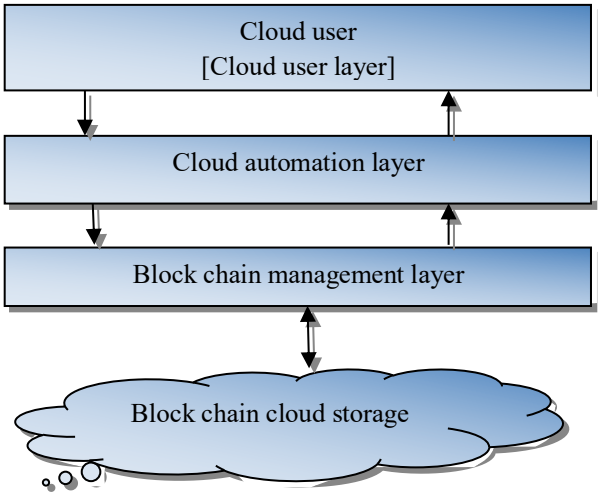

Fig. 1. Block chain cloud architecture

Figure 1 define the control and manage the cloud security system on private data environment. There are four layers used for this architecture.

A. Cloud User Layer

The most noteworthy layer, known as the cloud client layer, is comprised of individuals, affiliations, and so on who need admittance to cloud organizations or have to recuperate their delicate data in the cloud.

B. Cloud Automation Layer

Different cloud clients have different solicitation needs. The solicitations are gathered during the checking stage and are shipped off the investigation stage. In the examination stage, the solicitation is dissected as far as what sort of administration the client is mentioning and what its help is out and other security and protection prerequisites. The following stage is the arranging stage, where the reaction is booked in light of the client's solicitation. To meet explicit client needs, Venture Network utilizes an information base that rundowns strategies, administration level arrangements, and evaluating for all cloud administrations advertised. In the execution stage, the reaction is given to the cloud client following the client's particular prerequisite.

C. Block chain Management Layer

The third layer is the blockchain, the dashboard layer, which manages the cloud and works as a controller for the cloud association. Blockchain is the groundwork of this framework as it offers many features like access control, security, insurance, etc. Each cloud client can see every one of the organizations that the cloud gives, which are the cloud courses of action and what is their organization level. Contracts, fulfillment. These utilization cases incorporate open shared record, contract, shared agreement, and crypto. The blockchain dashboard layer is the groundwork of this construction as it manages all framework layers utilizing the blockchain capabilities.

D. Secure Data Storage Layer

The fourth layer is the limit of the Cloud. The dispersed stockpiling layer is a blockchain-empowered capacity layer, so the disseminated stockpiling layer furnishes security by staying aware of characterization, dependability, and openness. Data put away in the blockchain cloud is extremely durable and is created utilizing cryptographic methodologies, for example, hashing, encryption/decoding, and PC stamping to safeguard data.

2. Related Works

Blockchain is a coordinated synopsis that likewise stores data in a standard vault and is intended to be hard to utilize freely, since individuals of the affiliation save and affirm the chain of blocks. Each block comprises of a body and a header. The header contains the hash upsides of the current and past blocks, and the nonce. The information in the block is recovered from the server through the referenced plan. Since the hash values put away in each neighbor in the chain are impacted by the benefits of the past blocks, it is without a doubt a test to misshape and change the chose data [2].

The feature of the straightforwardness of the Blockchain is gotten through the multiplying time of the trade. As referenced over, all trades are considered any of the machines on the Blockchain organization. Every one of the clients can see every one of the trades, which additionally implies that each activity is displayed to the clients of the Blockchain, for instance, it is simple [3].

The HASBE scheme comprises of a multitier structure for application clients utilizing a CP-ASBE assignment technique. The HASBE structure favors composite credits because of the mix of dynamic and dependable capabilities and takes into serious areas of strength for account refusal because of numerous regard individuals [4].

More *et al*., [5] recommended a security for the information in the cloud utilizing the trait driven key total cryptographic framework. To check the document put away in the cloud, the framework

utilizes a secret entrance key and accessible watchwords. While recuperating the record, it requires an additional key to encode and get to a specific document from the information store. For a specific local area, the hidden entryway key is openly accessible, yet admittance to the collected key relies upon the data proprietor's qualities.

Sukhodolskiy *et al*., [6] offered a system to get to information put away in untrusted conditions, ie distributed storage. For instance, the information will be put away safely in the cloud, eg media records, logs, and so on, where the data that the document perceives is open on the blockchain.

Wöhrer *et al*., [7] have illustrated six plan designs, specifically, as far as possible example, the hindrance design, the mutex design, the equilibrium design, the check impact collaboration design, and the crisis stop design which they take care of safety issues while coding savvy contracts in Strength. These examples take care of the issue of execution control being lost after agreement execution, because of the Ethereum sandbox execution climate.

No one requirements admittance to your information until you permit it. Security is the capacity of an individual or gathering to seclude themselves or to find data about themselves specifically. It likewise engages clients to control their information when information is put away and observed in the cloud, and forestalls robbery, misuse, and unapproved resale [8].

The cloud was created to make it simple for your clients/associations by offering types of assistance through different organization models like public, private, local area and crossover. In any case, as outsiders (cloud specialist co-ops) gain control, trust, security, and vulnerability in the cloud increment and the individual control of the client/occupant of the cloud is much lower. The CSP and the TPA are not gatherings of complete certainty [9, 10].

Rong *et al*., [11] furnished a security system structure with Cloud SLA to cover cloud security perspectives. A large portion of the work in progress manages overseeing SLA certificates for the client. In use Blockchain to keep steady over the effortlessness of Cloud SLAs, Cloud Client Arrangements, and Information Saved in the Cloud. Affirm the good judgment of associating with Blockchain in the cloud by separating and isolating different security prerequisites and non-utility requirements in Blockchain and cloud.

Almorsy *et al*., [12] have proposed a model-based security plan technique that utilizes the framework portrayal model made at configuration time and the house structure model made at runtime to accomplish runtime security capacities for security applications. Programming. In any case, his way of thinking is nonsensical in cloud conditions, where various applications ought to fulfill near security needs, since even an update of his model requires the update of all designs connected with it.

Kertesz *et al*., [13] have presented SLA-based help virtualization electronic administration association designing considering the autonomous MAPE-K computation. Notwithstanding, their designing really incorporates the expensive life pattern of SLAs.

All copies of the record are in a condition of concordance, and all cloud clients can see a copy or comparable type of the record. The record will contain the ongoing organizations utilized by the cloud, the SLAs, the procedures and how much information the executive’s utilization of each cloud client. Cloud clients sync their record on the possibility of diggers in Bitcoin [14].

With regards to limitless handling resources, pay all the more just as expenses, utilization, cost contest, execution, and adaptability emerge, brought together cloud is better, while decentralized blockchain is more negative. Aside from that, the underlying systems are feebly connected [15].

Cloud-based EHR sharing arrangement has brought numerous accommodations, yet cloud centralization opens up certain dangers to information security and protection power outages. Blockchain improvement ought to be viewed as a promising solution to tackling these issues because of its remarkable properties of inundation, mystery, alter clear, and conviction [16].

In any case, there has been no agreement on the most proficient method to create, disperse, and approve dependable ads in such a problematic remote climate. Security and protection, the motivation instrument, and asset mix are critical difficulties for promotion age and dispersal. In this article, a safe and solid promotion conveyance conspire for Area Based Help (LBS) application on VANET is understood [17].

To urge one to report different violations, the legal division frequently leases separate distributed storage spaces to get the important proof of the complainants. Since cloud clients don't control the information transferred, the uprightness of distant information is vital. Public cloud reviewing permits an examiner to consistently confirm the honesty of re-appropriating information in the interest of clients, without recovering the whole information document [18].

Over the course of the last ten years, blockchain innovation has developed and become suitable for different applications past the area of money. Notwithstanding, because of the intricacy of blockchain innovation, it is frequently troublesome and expensive for most designers or groups to construct, keep up with, and screen a blockchain network that upholds their applications [19].

Public audit plans for disseminated capacity systems have been widely researched because of the rising significance of information decency. A third-party auditor (TPA) knows about plans for public survey to really take a look at the decency of the appropriated data for clients. To go against unsafe TPAs [20].

Specifically, EFPB incorporates various cryptographic design blocks, chiefly: one-way gatherer (RSA-based development), area stowing away, and symmetric encryption. Then assess EFPB's show to show that it is more viable and lower cost than other contending plans, alongside introducing a definite rundown of elements [21].

Network capacity administrations have helped endless clients across the world because of the astounding elements of comfort, economy and high accessibility. As a solitary specialist organization isn't generally sufficiently solid, more complicated multi-distributed storage frameworks are being created to moderate the gamble of information defilement. While an information review plot in multi-distributed storage is as yet expected to assist clients with affirming the respectability of their reevaluated information [22].

Because of their wide availability, cloud administrations are helpless against assaults. Information altering is a serious danger to information respectability that can happen in distributed computing, a generally new contribution under the haze administrations umbrella. Information can be messed with, and malignant entertainers could utilize this for their potential benefit [23].

3. Proposed Methodology

Cloud innovation is maybe the present most obvious and important development. Conveyed capacity has led to an electronic stockpiling plan that involves various servers in different regions to safely store data. Lately, appropriated capacity has become packed in different regions and has turned into a quick test for local area limit. The cloud gives the data stockpiling administration that permits the data proprietor to store their data in the cloud and permit admittance to the affiliations that need it.

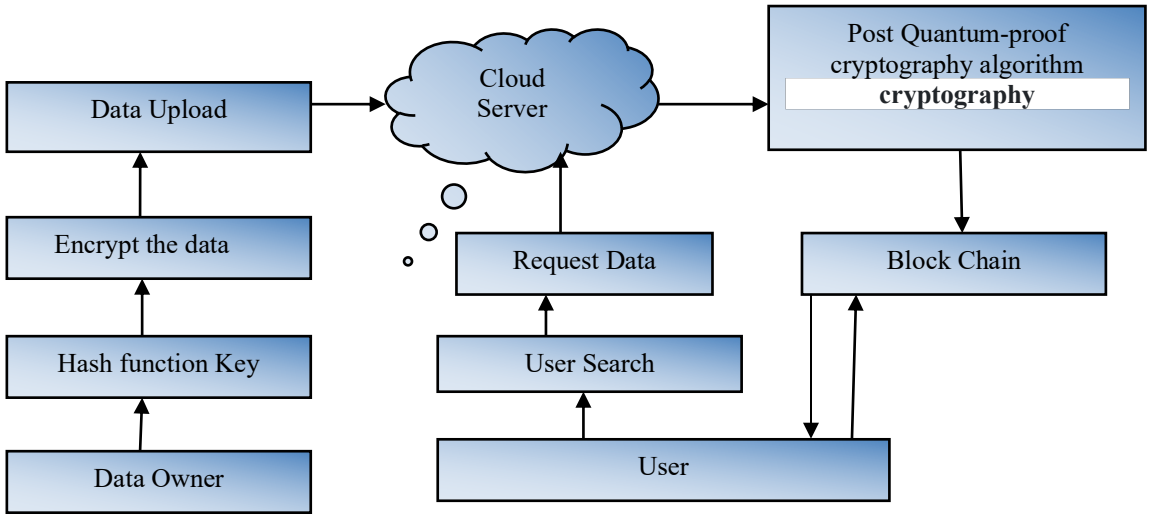

Fig. 2. Block Chain Based Proposed Architecture

Figure 2 defines the associations with arrive at the reports will be put away in the blockchain. From the start, the information proprietor will move the documents through the cloud in an encoded structure. The reports will be coded utilizing the Quantum confirmation system. These documents can be decoded utilizing the extra key given by the proprietor of the data. The client who requirements to get to the reports put away in the cloud should at first affirm his recognizable proof. After affirmation, the client looks into the normal record by utilizing a slogan look for certain reports. The proprietor of the data will share the public key for buried admittance of each record just with those clients that are embraced by the proprietor of the data.

A. SHA-3 512 Hash function algorithm

A hash is a numerical capability that works on two blocks of information of a proper size to make a hash code. This hash capability is important for the hash calculation. The size of each block of information shifts relying upon the calculation. Regularly, block sizes are from 128 pieces to 512 pieces. The representation beneath exhibits the hash capability. A hash capability is a numerical capability that transforms a numeric info esteem into one more packed numeric worth. The contribution to the hash capability is of erratic length, however the result is constantly fixed-length. The model hash capabilities for Figure 3 are displayed underneath.

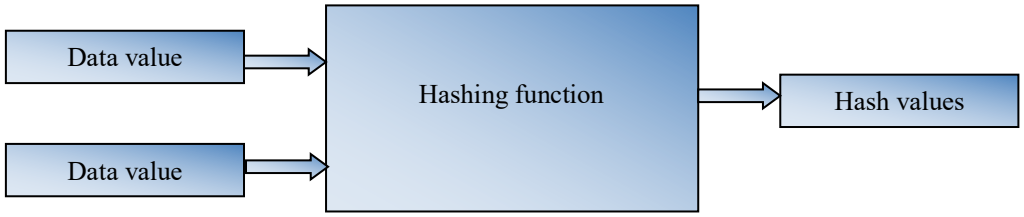

Fig. 3. Mathematical Function of Hash Function

Figure 3 portrays the effect of heavy slippage bringing about essentially various hashes for two messages that change by even a solitary piece of data. Unequivocally comprehend the contrast among hashing and calculation. The hash capacity makes a hash code by dealing with two fixed-length blocks of twofold data. The hash calculation is a circle to utilize the hashing limit, deciding how the message will be parted and how the outcomes of past message blocks will be rectified.

SHA3-512 hash algorithm 64 bit values of the function and 256 bit has been 20 round testing but 512 have been 80 round testing the hashing function because values support for more secure. In this SHA3-512 algorithm fly the 80 round of hash function, the following equation generate the signature.

$$r = \left\langle \langle g^{k} \rangle_{p} \right\rangle_{q} \quad (1)$$

$$S = \left\langle \langle k^{-1} + Xr \rangle_{q} \right\rangle \quad (2)$$

Where

$g = \left\langle \langle h^{p-1/q} \rangle_{p} \right\rangle$, 1<h<p-1, and 0<k<q randomly selected k, L m = 64 for any integer m, q is a prime, $2^{159} < q < 2^{260}$ x is a private key randomly generated, 0 < < x q; $M'' + Xr$ is the message M

$$v = \left\langle \langle g^{u1} g^{u2} \rangle_{p} \right\rangle_{q} \quad (3)$$

If $v = r'$ is message verified, be noted that y, g, p, and q are transparent to both the signatory and the receiver.

Initialize:

$A = H_0, B = H_1, C = H_2, \text{and } E = H_4$
$A_{t+1} = T$ (4)

Perform 80 rounds; for tt t = 0; 80; < ++ ;

for $t < 16$, ... W_t=W_t and for $t > 16$
$W_{t=S^1}($ $W_{t-16} \oplus W_{t-14} \oplus W_{t-8} \oplus W_{t-3}$ (5)

Final Adds

$$H_0 = H_0 + A_1 H_1 = H_1 + B_1 H_2 = H_2 + C$$

$H_3 = H_3 + D, H_4 + E$ (6)

For (4) – (6) above, + denotes addition with modulation reduction

$M'' = SHA - 3(M) \quad = \{H_0, H_1, H_2, +H_4\}$ (7)

To process the round word (Wt), the information is sectioned into 512-digit blocks. The last block is loaded up with "1" and a few "0"s and the information length to finish the 512-cycle block size. M'' is the message diggest key .

B. Post Quantum-proof cryptography algorithm

Post Quantum-proof cryptography algorithm is used strongly encrypt the data values and decrypt the values. Our applying the Post Quantum-proof cryptography algorithm for message M''. The following the encryption of the plaint text P and C is chipper text, and then encryption.

$$C = p^a \bmod M'' \quad (8)$$

And at decryption side

$$P = C^b \bmod M'' \quad (9)$$

M'' is a very large number, created during key generation process. Here a and b is the exponent values.

4. Result and Discussion

The block chain is an essential for security of distributed system in cloud storage. The proposed system have developed using .Net programing and Microsoft sqlserver based web application has been initialized. Our most need for cloud security is most important of the user application, security initialized using Quantum-proof cryptography algorithm based encryption and decryption is most powerful for secure communication for user application. The proposed system compare with various algorithm are SHA1, SHA256, MD5 but best result of the performance is Quantum-proof cryptography algorithm. The performance are based on encryption and decryption, power consumption, latency, security. The table 1 defines the encryption and decryption performances.

Table 1
Define The Encryption Performances

Methods	Encryption (m/sec)
SHA1	580ms
SHA256	480ms
MD5	27ms
Proposed	15ms

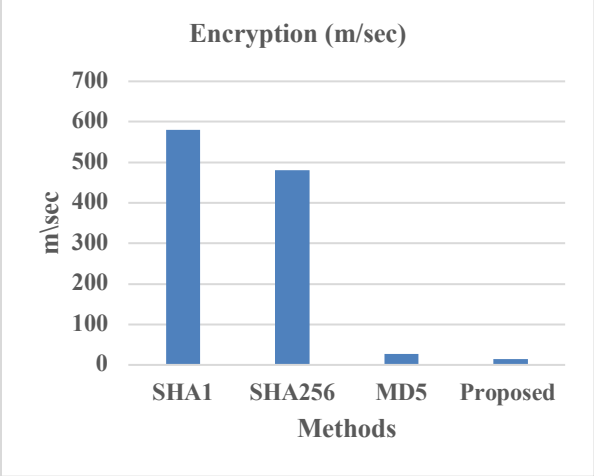

Fig. 4. Encryption performance

Figure 4 discuss about the encryption performance compared to various algorithm, the SHA1 algorithm is better than SHA256, and SHA256 is better than MD5 but finally better for proposed of Post Quantum-proof cryptography algorithm is 15m/sec for encryption time.

Table 2 and Figure 5 discuss about the power consumption performance compared to various algorithm, the SHA1 algorithm is better than SHA256, and SHA256 is better than MD5 but finally better for proposed of Post Quantum-proof cryptography algorithm power consumption is 11(Wh).

Table 2
Define the power consumption performances

Methods	Power consumption (Wh)
SHA1	17.5
SHA256	14.5
MD5	13
SHA-3(proposed)	11.5

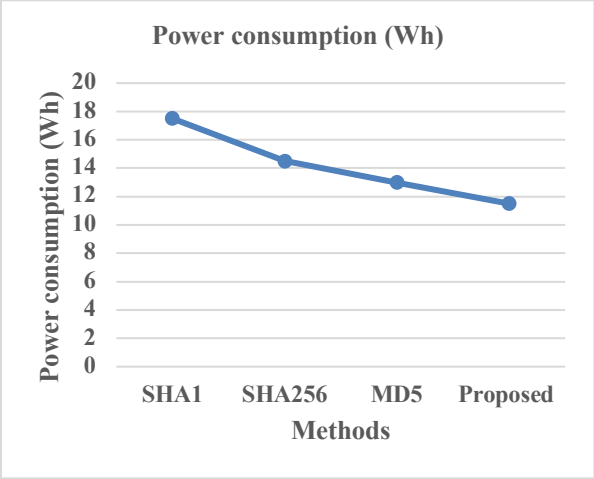

Fig. 5. Power consumptions performance

Table 3 and Figure 6 discuss about the Latency performance compared to various algorithm, the SHA1 algorithm is better than SHA256, and SHA256 is better than MD5 but finally better for proposed of Post Quantum-proof cryptography algorithm Latency performance is 78 m/sec.

Table 3
Define The Latency Comparison Performances

Methods	Latency Comparison(m/sec)
SHA1	60
SHA256	62
MD5	74
SHA-3(proposed)	78

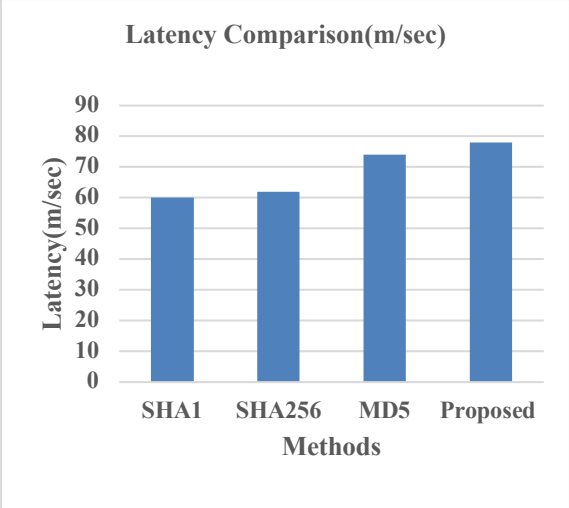

Fig. 6. Latency performance

Table 4 and Figure 7 discuss about the security performance compared to various algorithm, the AES algorithm is better than DES is 78 %, and IDEA is 82 % and MD5 is 89% but finally better for proposed of Post Quantum-proof cryptography algorithm security performance is 98%.

Table 4
Define The Block Chain Security Comparison Performances

Methods	Performance (%)
AES	78
DES	82
IDEA	89
Proposed	98

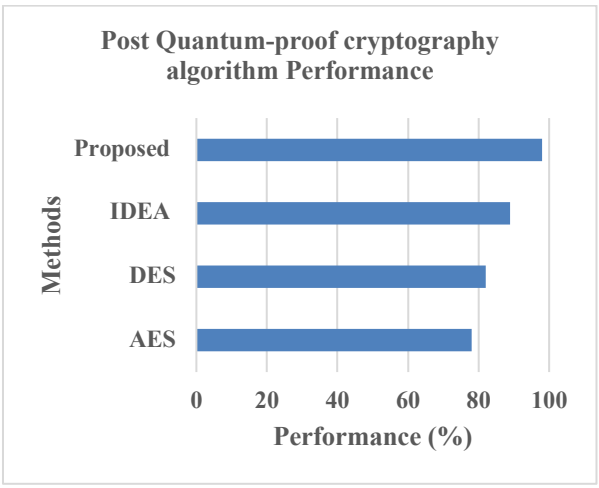

Fig. 7. Security performance

5. Conclusion

The cloud is a distributed network and various functions have been functioning the network. the function are data storage and data sharing and distributed but problem for need the security for encryption and decryption, security enhanced using block chain technology based cryptography system. The new proposed system algorithm is Post Quantum-proof cryptography algorithm is better

for security initiate block chain technology. The performance is based on encryption is performance is 15/m/sec and decryption and power consumption performance is 11.5 (Wh) and latency performance is 78 m/sec and security performance are 98%. Future will be increase the performance most powerful block chain algorithm

References

[1] Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. "An overview of blockchain technology: Architecture, consensus, and future trends." In *2017 IEEE international congress on big data (BigData congress)*, pp. 557-564. Ieee, 2017. https://doi.org/10.1109/BigDataCongress.2017.85

[2] Park, Jin Ho, and Jong Hyuk Park. "Blockchain security in cloud computing: Use cases, challenges, and solutions." *Symmetry* 9, no. 8 (2017): 164. https://doi.org/10.3390/sym9080164

[3] Golosova, Julija, and Andrejs Romanovs. "The advantages and disadvantages of the blockchain technology." In *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*, pp. 1-6. IEEE, 2018. https://doi.org/10.1109/AIEEE.2018.8592253

[4] Nimje, Anup R., V. T. Gaikwad, and H. N. Datir. "Attribute-based encryption techniques in cloud computing security: an overview." *Int. J. Comput. Trends Technol* 4, no. 3 (2013): 419-422.

[5] More, Pooja, and D. G. Harkut. "Cloud data security using attribute-based key-aggregate cryptosystem." In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 855-861. IEEE, 2016. https://doi.org/10.1109/WiSPNET.2016.7566253

[6] Sukhodolskiy, Ilya, and Sergey Zapechnikov. "A blockchain-based access control system for cloud storage." In *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 1575-1578. IEEE, 2018. https://doi.org/10.1109/EIConRus.2018.8317400

[7] Wohrer, Maximilian, and Uwe Zdun. "Smart contracts: security patterns in the ethereum ecosystem and solidity." In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, pp. 2-8. IEEE, 2018. https://doi.org/10.1109/IWBOSE.2018.8327565

[8] Rao, B. Thirumala. "A study on data storage security issues in cloud computing." *Procedia Computer Science* 92 (2016): 128-135. https://doi.org/10.1016/j.procs.2016.07.335

[9] Li, Jingwei, Chunfu Jia, Jin Li, and Xiaofeng Chen. "Outsourcing encryption of attribute-based encryption with mapreduce." In *Information and Communications Security: 14th International Conference, ICICS 2012, Hong Kong, China, October 29-31, 2012. Proceedings 14*, pp. 191-201. Springer Berlin Heidelberg, 2012. https://doi.org/10.1007/978-3-642-34129-8_17

[10] Tang, Jun, Yong Cui, Qi Li, Kui Ren, Jiangchuan Liu, and Rajkumar Buyya. "Ensuring security and privacy preservation for cloud data services." *ACM Computing Surveys (CSUR)* 49, no. 1 (2016): 1-39. https://doi.org/10.1145/2906153

[11] Rong, Chunming, Son T. Nguyen, and Martin Gilje Jaatun. "Beyond lightning: A survey on security challenges in cloud computing." *Computers & Electrical Engineering* 39, no. 1 (2013): 47-54. https://doi.org/10.1016/j.compeleceng.2012.04.015

[12] Almorsy, Mohamed, John Grundy, and Amani S. Ibrahim. "Mdse@ r: model-driven security engineering at runtime." In *Cyberspace Safety and Security: 4th International Symposium, CSS 2012, Melbourne, Australia, December 12-13, 2012. Proceedings 4*, pp. 279-295. Springer Berlin Heidelberg, 2012. https://doi.org/10.1007/978-3-642-35362-8_22

[13] Kertész, Attila, Gabor Kecskemeti, and Ivona Brandic. "An interoperable and self-adaptive approach for SLA-based service virtualization in heterogeneous Cloud environments." *Future Generation Computer Systems* 32 (2014): 54-68. https://doi.org/10.1016/j.future.2012.05.016

[14] Aljoumah, Eman, Fajer Al-Mousawi, Imtiaz Ahmad, Maha Al-Shammri, and Zahraa Al-Jady. "SLA in cloud computing architectures: A comprehensive study." *Int. J. Grid Distrib. Comput* 8, no. 5 (2015): 7-32. https://doi.org/10.14257/ijgdc.2015.8.5.02

[15] Rimba, Paul, An Binh Tran, Ingo Weber, Mark Staples, Alexander Ponomarev, and Xiwei Xu. "Comparing blockchain and cloud services for business process execution." In *2017 IEEE international conference on software architecture (ICSA)*, pp. 257-260. IEEE, 2017. https://doi.org/10.1109/ICSA.2017.44

[16] Wang, Yong, Aiqing Zhang, Peiyun Zhang, and Huaqun Wang. "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain." *Ieee Access* 7 (2019): 136704-136719. https://doi.org/10.1109/ACCESS.2019.2943153

[17] Li, Xincheng, Xinchun Yin, and Jianting Ning. "Trustworthy Announcement Dissemination Scheme With Blockchain-Assisted Vehicular Cloud." *IEEE Transactions on Intelligent Transportation Systems* 24, no. 2 (2022): 1786-1800. https://doi.org/10.1109/TITS.2022.3220580

[18] Zhao, Jie, Hejiao Huang, Chonglin Gu, Zhongyun Hua, and Xiaojun Zhang. "Blockchain-assisted conditional anonymity privacy-preserving public auditing scheme with reward mechanism." *IEEE Systems Journal* 16, no. 3 (2021): 4477-4488. https://doi.org/10.1109/JSYST.2021.3125835

[19] Zheng, Weilin, Zibin Zheng, Xiangping Chen, Kemian Dai, Peishan Li, and Renfei Chen. "Nutbaas: A blockchain-as-a-service platform." *Ieee Access* 7 (2019): 134422-134433. ttps://doi.org/10.1109/ACCESS.2019.2941905

[20] Shu, Jiangang, Xing Zou, Xiaohua Jia, Weizhe Zhang, and Ruitao Xie. "Blockchain-based decentralized public auditing for cloud storage." *IEEE Transactions on Cloud Computing* 10, no. 4 (2021): 2366-2380. https://doi.org/10.1109/TCC.2021.3051622

[21] Zou, Xiang, Peng Zeng, and Huajie Cheng. "EFPB: Efficient Fair Payment Based on Blockchain for Outsourcing Services in Cloud Computing." *IEEE Access* 11 (2023): 30118-30128. https://doi.org/10.1109/ACCESS.2023.3261560

[22] Zhang, Cheng, Yang Xu, Yupeng Hu, Jiajing Wu, Ju Ren, and Yaoxue Zhang. "A blockchain-based multi-cloud storage data auditing scheme to locate faults." *IEEE Transactions on Cloud Computing* 10, no. 4 (2021): 2252-2263. https://doi.org/10.1109/TCC.2021.3057771

[23] Awadallah, Ruba, Azman Samsudin, Je Sen Teh, and Mishal Almazrooie. "An integrated architecture for maintaining security in cloud computing based on blockchain." *IEEE Access* 9 (2021): 69513-69526. https://doi.org/10.1109/ACCESS.2021.3077123