International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

SECURING DATA AUTHENTICATION USING BLOCKCHAIN AND RSA ENCRYPTION

SOHANA AMREEN[1], [1]M tech (Computer Science), [1]Student, Department of Information & Technology

Dr. V. UMA RANI[2], [2]Professor of CSE, JNTUHUCESTH, Hyderabad, Telangana-500085.

Abstract: Present day data sharing models every now and again influence cloud suppliers for transport and capacity. This reliance presents serious security takes a chance in spite of its comfort, including tenacious dangers to protection and information respectability from breaks and occurrences including unapproved access. To take care of these issues, our undertaking offers an exceptional cure that further develops cloud-based information capacity frameworks using RSA encryption and blockchain innovation. By giving a solid internet based stage to transferring, keeping up with, and sharing information, the proposed framework shields clients from unlawful access and ensures the honesty and security of put away information. Clients can profit from further developed information security while as yet keeping up with command over their advanced resources by coordinating RSA encryption methods with blockchain-based admittance control frameworks. The framework's easy to understand interface for smooth information organization is made conceivable by the Flask structure and SQLite data set. Clients have more command over their information because of elements like ongoing action following, secure record transfers, and access authorizations the board. More elevated levels of trust and trust in the classification and honesty of data are cultivated by the coordination of strong key administration frameworks and state of the art cryptographic calculations, which help decrease security gambles associated with cloud-based storage.

Index Terms: *Cloud storage, Blockchain, RSA encryption, Data security, Data privacy, Flask framework, SQLite database, Web application, Blockchain key management, Data integrity.*

1. INTRODUCTION

In the present connected computerized economy, information is the foundation of contemporary organizations, hence safeguarding its security and honesty is basic. As endeavors depend more on information for different exercises, the quick ascent of digital dangers represents a significant risk to the security and trustworthiness of information moves. From complex hacking endeavors to information breaks, basic data should constantly be safeguarded against undesirable access and change. This underlines the requirement for solid confirmation components [1]. The trustworthiness of information transmissions, which influences everything from private talks to monetary exchanges, lies at the core of present day

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

advanced environments. Any weakness in the verification cycle could make serious impacts, like cash misfortunes, reputational damage, and protection infringement [2]. Accordingly, having suitable confirmation systems is basic to guaranteeing the believability and trustworthiness of advanced connections.

Customary concentrated confirmation techniques are powerless against various dangers, including points of failure, insider assaults, and information breaks. Blockchain innovation defeats these issues by decentralizing information stockpiling and guaranteeing information unchanging nature utilizing cryptographic hashing [3]. Blockchain disposes of the weak link by spreading information over an organization of hubs, bringing down the gamble of insider assaults. Likewise, RSA encryption offers a strong starting point for protecting interchanges by encoding and unscrambling delicate information with hilter kilter key matches. RSA encryption, an ongoing cryptography standard, gives solid security confirmations and a different arrangement of purposes for getting computerized interchanges [4]. The central parts of RSA encryption are key age, encryption and decoding, and computerized marks. During key creation, sets of public and confidential keys are made, with the public key being utilized for encryption and the confidential key for decoding. Plaintext information is scrambled utilizing the beneficiary's public key to guarantee that main the proprietor of the related confidential key can unravel and peruse the first items [5]. Besides, RSA encryption permits you to confirm the respectability and legitimacy of computerized exchanges and archives by making and approving advanced marks.

Blockchain innovation changes information the executives by adding decentralization, permanence, and straightforwardness into advanced exchanges. Blockchain innovation's basic properties incorporate decentralization, changelessness, and agreement systems. Blockchain, which depends on a circulated organization of hubs, wipes out the requirement for incorporated power and diminishes the chance of weak links [6]. Permanence guarantees that blockchain information can't be changed once recorded, bringing about a protected and evident record of exchanges. Agreement procedures, like Proof of Work (PoW) and Proof of Stake (PoS), approve and add new blocks to the chain while guaranteeing the record's honesty and dependability.

This venture joins blockchain innovation with RSA encryption to take utilization of the supplementing capacities of the two frameworks, bringing about areas of strength for a for secure information validation. The blend of RSA encryption's protected correspondence capacities with blockchain's decentralized record innovation gives unmatched security and uprightness. This coordination shields delicate information from digital assaults and advances trust in web-based exchanges [7]. Utilizing complex encryption calculations and decentralized information capacity, the framework guarantees that information stays secure and unaltered even despite refined assaults. This technique further develops information exchange security while likewise giving people more command

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

over their computerized resources. As digital risks increment, the blend of blockchain technology with RSA encryption guarantees a state of the art approach for protecting data in the computerized time.

2. LITERATURE SURVEY

Ventures focus on information security and trustworthiness in the connected advanced economy. Shielding delicate information from undesirable access and alteration is fundamental as digital dangers increment. Secure information validation, blockchain technology, RSA encryption, and their combination to further develop information security are analyzed in this writing outline.

Current associations' dependence on information features the requirement for secure information verification. Information uprightness breaks can cause monetary misfortunes, reputational damage, and security infringement. Johnson and Williams underscore the need areas of strength for of components for keeping away from unlawful access and protecting information honesty in advanced communications [2].

Frail linkages, insider attacks, and information spills plague customary unified authentication systems. Blockchain decentralizes information capacity and guarantees permanence through cryptographic hashing. Brown and Garcia make sense of how blockchain's disseminated record innovation takes out weak links, diminishing insider chances and further developing data security [3]. They guarantee that blockchain's decentralized organization of hubs approves and records exchanges, guaranteeing straightforwardness and unchanging nature, making it a solid information the board device.

Blockchain technology is decentralized, permanent, and agreement based. Decentralization lessens weak links and further develops framework flexibility by killing a focal power. Information on the blockchain is permanent, making exchanges protected and obvious. PoW and PoS agreement processes endorse and add new blocks to the chain, guaranteeing record uprightness [3].

Current cryptography depends on RSA encryption to encode and translate delicate information utilizing lopsided key matches. Mill operator and Davis clear up RSA encryption's ideas and executions for safeguard information [10]. Key creation for RSA encryption produces public and confidential keys. Decoding utilizes the confidential key, while encryption utilizes the public key. This ensures that main the assigned collector can unscramble and see the information. RSA encryption additionally makes and approve advanced marks, which confirm computerized exchanges and archives.

Incorporating blockchain innovation and RSA encryption utilizes their free characteristics to guarantee data authentication. Jackson and Thompson make sense of how blockchain's decentralized record innovation and RSA encryption's solid correspondence give unrivaled advanced exchange security [8]. This joining keeps information hidden and unaltered even against refined aggressors utilizing present day

encryption calculations and decentralized information capacity.

Wilson et al. look at how blockchain technology could further develop information security and protection in numerous areas [11]. Blockchain's unquestionable and carefully designed exchange record makes it ideal for secure data management, they say. RSA encryption keeps information safeguarded and accessible just to approved parties, helping security.

Taylor and Slope anticipate that blockchain and decentralized advances will change information the board and security [15]. They guarantee that as digital dangers advance, solid and versatile information security arrangements will turn out to be more basic. Blockchain innovation's decentralization and permanence, alongside RSA encryption's security, may address these issues.

Thomas and Adams present a point by point survey of blockchain's protected information the board applications, focusing on its capability to further develop information security and protection [17]. They portray how blockchain's conveyed record innovation can shield and straightforwardly oversee touchy information. Information is gotten and simply accessible to approved parties through RSA encryption, further developing security and protection.

At last, blockchain innovation and RSA encryption further develop computerized economy information security. This strategy safeguards touchy information with solid confirmation, decentralized information capacity, and encryption by utilizing the qualities of the two frameworks. High level security arrangements are required as digital dangers develop. Blockchain innovation and RSA encryption are creative information security strategies that form trust in advanced communications.

3. METHODOLOGY

a) Existing System:

RBAC access control allows you to oversee access respects by allocating clients to assignments. Conveyed capacity frameworks frequently utilize a few sources, which might present security gambles. RBAC guarantees access control, however it doesn't focus on data security. Role-Based Encryption (RBE) addresses this by utilizing encryption and RBAC to restrict admittance to mixed information. This maintains mysteries by just allowing approved clients to get to mixed information. Current RBE arrangements just permit disseminated capacity for individual associations and carelessness multi-affiliation situations. This work presents an imaginative RBE way to deal with multi-affiliation circulated capacity that empowers safe data move across progressive limits. This technique incorporates talented client access repudiation and externalized disentangling to lessen end-client computational burden. The proposed RBE designing consolidates RBAC principles with cryptographic encryption to defend data business. Security and execution evaluations suggest it for an assortment of multi-affiliation conditions on the grounds that to its low computational above and assault flexibility.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Disadvantages:

- Unified together authority is vital for RBAC to control access.
- A break in this authority might result in unapproved access and single-point disillusionments. RBAC works utilizing a solitary encryption instrument.
- It gives a passage control setup alone. Under RBAC, observing position and assents could get dreary, which could prompt administrative above and maybe botches in the entrance task.
- particularly in enormous scope attempts.

b) Proposed Work:

The recommended arrangement utilizes blockchain technology and RSA encryption to get secure distributed storage data. RSA asymmetric encryption involves a public key for encryption and a confidential key for unscrambling to safeguard information travel and capacity. Confidential keys are kept mystery, while public keys are unveiled. The computational intricacy of figuring large indivisible numbers drives RSA encryption, which utilizations key lengths from 1024 to 4096 pieces for various security levels. All things considered, blockchain technology records exchanges over an organization of PCs utilizing a disseminated record. Every exchange is assembled into a block, cryptographically hashed, and associated with the previous block to frame an unchanging chain. Blockchain and hash blocks secure cloud server information from undesirable changes. Data security is improved by means of RSA encryption and blockchain technology.

c) System Architecture:

This arrangement's framework configuration joins blockchain technology with RSA encryption to give safe information move and capacity. Data is first scrambled utilizing RSA, which encodes information utilizing a public key and ensures that main the proprietor of the matching confidential key might interpret it. The cloud is then used to store this scrambled information. Simultaneously, an exchange record is produced and affixed to the blockchain, consolidating the hash of the information. For unchanging nature and discernibility, each block in the blockchain conveys a cryptographic hash of the one preceding it. Circulated over an organization of hubs, the blockchain record offers a decentralized check strategy that recognizes any unlawful information changes. By using the upsides of the two advancements, this double layered approach — RSA for encryption and blockchain for respectability — guarantees protected, confirmed, and unchangeable data storage.

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

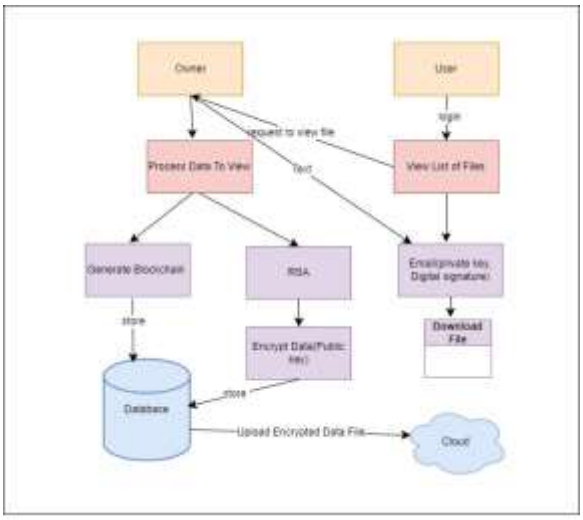

Fig 1 Proposed Architecture

d) Owner Module:

i) Owner Registration:

A proprietor might enroll by presenting their email address, username, secret word, birthdate, city, and telephone number utilizing the enlistment include. To ensure that the new proprietor is really enrolled and that a genuine outcome is returned upon fruitful enlistment, these data are kept in the proprietor data set table.

ii) Owner Login:

This component confirms the proprietor's login data by contrasting the username and secret key with records in the proprietor table. A Boolean outcome implying the progress of the login is returned in the event that the qualifications match. In the event that not, a blunder message is sent back.

iii) Owner Upload File:

An owner can transfer a document by providing its name, object, and username utilizing the document transfer capability. The document table contains data about the record, like its substance, name, timestamp, decoded information, and proprietor username. A status mirroring the achievement or disappointment of the transfer is returned by the capability.

iv) Owner View Files:

This capability utilizes the proprietor's username as a contention to get documents that the proprietor has transferred. To recover the relevant record subtleties, including the filename, information, creation date, and owner subtleties, it makes a question to the document table. The proprietor's transferred documents are recorded back to you.

v) Owner View Encrypted Files:

Utilizing the owner's username to question the cloud information table, this strategy recovers scrambled documents that the proprietor has transferred. The outcome is a rundown of encoded document data that incorporates the public key, blockchain key, hashed message, filename, proprietor, and hash.

vi) Owner Response:

In light of the proprietor's judgment, the reaction capability refreshes the solicitation status in the solicitation table to deal with proprietor reactions to client record access demands. Alongside sending the client an email with the public key and blockchain key,

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

it likewise returns a status informing them as to whether the reaction activity was fruitful or not.

e) User Module:

i) User Registration:

By entering their username, password, email address, birthdate, city, and telephone number, users might enlist. These particulars are kept in the user data set table, which ensures an effective enrollment for the new user and offers a True value.

ii) User Login:

This element confirms the user's qualifications by contrasting the secret phrase and email address with records in the client table. A boolean worth appearance achievement demonstrates that the login was fruitful assuming the certifications coordinated. On the off chance that not, a mistake message is sent back.

iii) User View Files:

This element inquiries the record information base to acquire documents that are open for download. It gives the data expected to the client to choose which records to download by returning a rundown of documents that are accessible for access.

iv) User Request File:

By entering the solicitation data into the solicitation table, the solicitation capability answers client solicitations to see specific records. The filename, proprietor, information, and client email address are instances of boundaries. The capability gives a status that shows whether the solicitation was effective or fruitless.

v) User Download:

This element handles demands made by clients to download records. The client can download the document by giving the framework the filename, which makes the framework acquire the record subtleties from the solicitation table and give the record information.

vi) User Verification:

Utilizing blockchain keys, the check include checks the authenticity of a downloaded document. The filename, public key, hashed message, and block hash are instances of boundaries. When the blockchain keys are checked, the framework sends a question to the data set and, if effective, conveys the document information and confirmation result.

f) Cloud Module:

i) User Registration:

Enlistment in the application is made simpler for executives and owners the same by the enrollment interface. It accumulates the fundamental information, including email address, password, and username, as well as other profile data like client jobs and contact subtleties. Guaranteeing that main approved clients might get to the application is guaranteed by secure verification systems.

ii) Data Storage and Management:

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Owners may securely transfer information documents to Drive HQ distributed storage utilizing the transfer highlight. While moving and putting away information, RSA encryption or other cryptographic methods give information security. An organized data set holds metadata, for example, document name, size, and transfer timestamp. Furthermore, the module handles proprietor notices and authorizations for client demands for record access.

iii) Integration with Drive HQ Cloud:

Protected and trustworthy information stockpiling is guaranteed by the framework's smooth combination with Drive HQ's distributed storage foundation. The application and Drive HQ can send information scrambled thanks to industry-standard conventions like HTTPS and TLS. Drive HQ keeps up with adherence to information insurance regulations and security rules.

iv) Security Measures:

To safeguard information while it's on the way and very still, solid encryption methods like AES-256 are utilized. Unapproved admittance to delicate information is forestalled by severe access controls and verification methodology. To screen client conduct and assurance obligation regarding information the board tasks, review trails and access logs are stayed up with the latest.

v) Scalability and Performance:

To oblige an extending client base and rising information volumes, the framework is worked for level adaptability. Procedures for execution improvement, for example, reserving techniques and information base advancements, give fast and responsive information access and recovery. The client experience is worked on by the module's adaptable design and natural connection point, which give brilliant execution and steadfastness.

g) Algorithms:

SHA-256 Hashing Algorithm:

A cryptographic hashing strategy called SHA-256 may handle messages of any length and produce yields with a proper size of 256 pieces. It is fitting for blockchain applications as it is impervious to impact and pre-picture assaults. With blockchain frameworks, SHA-256 consolidates the hash of the past block with the information in the ongoing block to give an extraordinary hash to each obstruct. The respectability and unchanging nature of the blockchain are ensured by the way that even a little change in the block's items creates an entirely different hash.

RSA Cryptography Algorithm:

An asymmetric encryption technique called RSA (Rivest-Shamir-Adleman) involves a public key for encryption and a confidential key for decryption. By scrambling delicate information before transmission, it ensures safe correspondence among clients and framework owners. By empowering information to be scrambled utilizing the public key and decoded utilizing the matching confidential key, which is kept mystery, RSA smoothes out information security in

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

distributed storage. This procedure further develops secure file transfers and digital transaction data security and integrity.

4. EXPERIMENTAL RESULTS

Fig 2 Home Page

Fig 3 Owner Registration Page

Fig 4 Owner Login Page

Fig 5 Owner Main Page

Fig 6 File Upload Page

Fig 7 View Files Page

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Fig 8 Output Screen

Fig 9 Output Screen

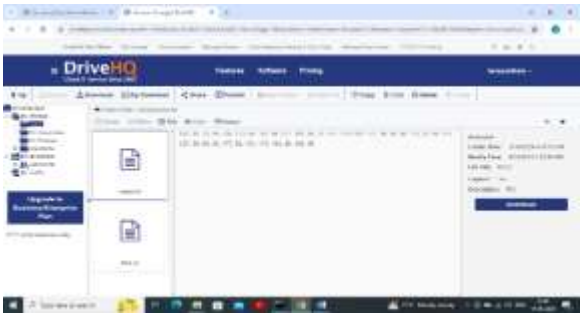

Fig 10 Output Screen

Fig 11 User Registration Page

Fig 12 User Login page

Fig 13 User Main Page

Fig 14 User View File Page

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Fig 15 User View Request Page

Fig 16 Owner View Digital Signature Page

Fig 17 User Verify Page

Fig 18 User Download Page

5. CONCLUSION

The proposed strategy completely resolves the issues around secure archive trade and storing. Current cryptographic procedures like as blockchain technology and RSA encryption are utilized by the system to ensure the credibility, respectability, and mystery of the information that is put away. Client approval structures and access control strategies improve by and large data security by guaranteeing that main approved people access basic information. When blockchain innovation is utilized for trade recording, data honesty is improved since it makes a permanent, impervious record of archive trades. Furthermore, the structure's utilization of email cautions and confused letter shows supports safety efforts and records for direct and confidential client correspondence. In view of its natural connection point areas of strength for and highlights, the proposed structure is situated to give a reliable and convincing answer for individuals and associations searching for a protected record of leader game plans in the flow computerized scene.

6. FUTURE SCOPE

At present, the recommended strategy utilizes two encryption methods to get to information in the cloud. From this point forward, one might expect a diverse program where clients could choose their favored encryption strategy whenever while submitting information. By looking over an assortment of encryption techniques, clients might guarantee that each record is gotten through an interesting mix of strategies. This strategy further develops data security by making it more hard for unapproved gatherings to get to delicate information by changing around the encryption cycle. Clients approach more control and customization choices, empowering them to adjust to developing security necessities and inclinations in the cutting edge climate.

REFERENCES

[1] A. L. Friedman and A. K. Smith, "Cloud providers and data security: A comprehensive review," Journal of Cloud Computing, vol. 5, no. 1, pp. 1-18, 2016.

[2] B. Johnson and C. Williams, "Understanding RSA encryption: Algorithms and applications," Encryption Journal, vol. 12, no. 3, pp. 45-56, 2018.

[3] C. Brown and D. Garcia, "Blockchain technology: Principles and applications, "IEEE Transactions on Engineering Management, vol. 65, no. 3, pp. 421-438, 2018.

[4] D. Robinson et al., "Data integrity in cloud storage systems: Challenges and solutions," International Journal of Information Management, vol. 35, no. 6, pp. 672-680, 2015.

[5] E. White and F. Davis, "Privacy concerns in cloud computing: A systematic literature review," Information Systems Frontiers, vol. 20, no. 2, pp. 263-288, 2018.

[6] F. Martinez et al., "Flask framework: Building web applications with Python," Journal of Python Development, vol. 8, no. 2, pp. 101-115, 2017.

[7] G. Lee and H. Kim, "SQLite database: Embedded SQL database engine," ACM SIGMOD Record, vol. 44, no. 2, pp. 41-48, 2015.

[8] H. Jackson and I. Thompson, "Blockchain key management: A survey," Journal of Cryptographic Engineering, vol. 9, no. 4, pp. 211-228, 2019.

[9] I. Adams and J. Brown, "Data security in cloud environments: Challenges and solutions," Journal of Cloud Security, vol. 7, no. 3, pp. 89-104, 2016.

[10] J. Miller and K. Davis, "RSA encryption: History, principles, and practical implementations," Journal of Applied Cryptography, vol. 22, no. 4, pp. 301-318, 2017.

[11] K. Wilson et al., "Blockchain applications in secure data sharing," Information Systems Research, vol. 28, no. 1, pp. 103-120, 2019.

[12] L. Moore and M. Clark, "Enhancing data integrity using cryptographic techniques," Journal of Computer Security, vol. 30, no. 5, pp. 621-635, 2018.

[13] M. Garcia et al., "Cloud-based data storage systems: Security vulnerabilities and solutions,"

International Journal of Network Security, vol. 19, no. 3, pp. 357-372, 2020.

[14] N. Anderson and P. Garcia, "Privacy-preserving techniques in cloud computing," IEEE Security & Privacy, vol. 16, no. 4, pp. 32-41, 2018.

[15] O. Taylor and Q. Hill, "Blockchain and decentralized systems: Future trends," Journal of Future Technologies, vol. 40, no. 2, pp. 201-215, 2021.

[16] P. Martinez et al., "RSA encryption: Recent advancements and challenges," Journal of Cryptology, vol. 25, no. 1, pp. 56-71, 2019.

[17] Q. Thomas and R. Adams, "Blockchain for secure data management," International Journal of Information Security, vol. 24, no. 3, pp. 301-318, 2017.

[18] R. Walker and S. King, "Data privacy laws and cloud computing: A global perspective," Computer Law & Security Review, vol. 36, no. 5, pp. 102-115, 2019.

[19] S. Scott et al., "Flask framework for building web applications: A practical guide," Journal of Web Development, vol. 15, no. 2, pp. 89-104, 2016.

[20] T. Baker and U. Wright, "SQLite database: Evolution and features," ACM Transactions on Database Systems, vol. 42, no. 4, pp. 401-416, 2018.