International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04609
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

A SECURE BLOCKCHAIN FRAMEWORK FOR COLLABORATIVE SERVICE

N VENKATESWARAN[1] PAMPATTI SRIVYSHNAVI[2] VARUKOLU SAIRAMAKRISHNA[3] JAGIRI MEGHANA[4] MANCHIKANTI RAKESH[5] VODDENENI NISHITH[6]

[1]Associate Professor, Department of CSE, Jyothishmathi institute of technology and science, Nustulapur, Karimnagar, T.S., India

[2,3,4,5,6]UG students, Department of CSE, Jyothishmathi institute of technology and science, Nustulapur, Karimnagar, T.S., India

venkateswaran.n@jits.ac.in, pampattisrivyshnavi@gmail.com, sairamakrishna.varkolu@gmail.com, jagirimeghana28@gmail.com, rakeshmanchikanti12@gmail.com, Nishithraovoddeneni@gmail.com

Abstract: With the rapid development of cloud computing, a large number of web services have been emerging quickly, which brings a heavy burden for users to choose the services they preferred. In order to suggest web services for users, recommendation algorithms are needed and many of them have been investigated recently. However, most of the existing recommendation schemes are based on centralized historical data, which may lead to single point of failure. Generally, the data contains a lot of sensitive information that cloud may expose the privacy of users, which makes most cloud platforms reluctant to share their own data. In order to solve the above issues, the secure data sharing among cloud platforms is necessary for better recommendation, which can maximize the profits. In this paper, we propose a blockchain assisted collaborative service recommendation scheme (*BC-SRDS*). Specifically, we adopt the ciphertext-policy attribute-based encryption (CP-ABE) algorithm to encrypt the data, which ensures the data confidentiality and realizes secure data sharing. Then, we utilize the blockchain to share data, such that the DoS attack, DDoS attack and single point of failure can be avoided. Meanwhile, the data integrity, tampering-proof of data are guaranteed through the blockchain. And we use locality-sensitive hashing algorithm to recommend the services for users. Finally, it is proved through the security analysis that *BC-SRDS* is capable of achieving data confidentiality, data integrity and tampering-proof. A series of experiments show that *BC-SRDS* achieves better recommendation accuracy compared with the existing schemes.

Key terms: Elliptic curve cryptography (ECC) Digital signature Micro grid, Fuzzy Logic Control (FLC), Pulse-Width Modulation (PWM), Renewable Energy, Converters.

I.INTRODUCTION

For the rapid development of the Internet and computer technology, a large number of network information services have entered people's daily life, providing users with many conveniences. Meanwhile, due to the rapid growth of Internet users, the information generated by users also presents an explosive growth, leading to the problem of ``information overload''. It is an important challenge for producers and consumers in today's society: for Internet service providers, it is very difficult for Internet service providers to select the services through user information quickly and make their services popular with the public. For Internet users, it is not easy to select the services they are interested in from the vast amount of information, which requires a lot of time and energy.

In order to solve above problems, a lot of recommendation algorithms have been proposed, among which collaborative filtering recommendation is a common method. It provides personalized recommendation for target user according to the scoring records of resources. Moreover, the algorithm has a good recommendation effect and is widely used in personalized sites, e-commerce, and other fields. Although the collaborative filtering recommendation algorithm has high recommendation accuracy, it still faces a series of challenges: the data used in the collaborative filtering recommendation algorithm is often stored

on the centralized server, so there is no historical data for new users or new items to refer to, and it may encounter cold start problem and cannot complete the recommendation. However, by collecting the data of users on different platforms, the problem of cold start can be solved effectively. For example, user *A* has called the services of Amazon and user *B* has called the services of IBM. If *A* and *B* are similar users, they can recommend services to *A* by analyzing the services of *B*, or recommend services to *B* by analyzing the services of *A*. Nonetheless, a malicious recommendation may lead to data abuse or privacy leakage issues. Therefore, in order to protect users' privacy information, Amazon and IBM are reluctant to share user data with each other. In this case, we cannot obtain similar users of new users, which greatly reduces the quality of recommendation. Besides, assume that two platforms agree to share data, and obtain the data from different platforms to improve the recommendation accuracy. But there still exists th e problem that the data stored in different distributed platforms greatly increases the communication overhead between cloud platforms, which cannot response quickly when online.

In order to solve the above problems, in this paper, we propose a novel block chain assisted collaborative service recommendation scheme with data sharing (*BC-SRDS*), with which every platform can share their data securely based on block chain. And locality sensitive hash (LSH) is an efficient dataw search algorithm that can quickly find similar data, therefore, the LSH is adopted to perform quick recommendation. The main contribution can be summarized as follows V

1) To the best of our knowledge, many recommendation algorithms are based on centralized data, but little of them adopt block chain to realize the recommendation. Moreover, it is difficult to combine distributed cloud platforms to share their data with each other for recommendation because of users' privacy. In order to realize better recommendation, in this paper, we introduce block chain to provide a secure sharing environment for accurate recommendation.

2) Different from most existing recommendation works, we adopt the CP-ABE (cipher text-policy attribute-based encryption) to promote the data sharing among the cloud platforms and combine block chain to ensure the security of data provenance, avoid the risk on the failure of single point, improve data integrity, and defend against DOS or DDOS attacks.

Based on the real distributed QOS (quality of service) dataset WS-DREAM,1 the experimental results show the effectiveness of *BC-SRDS*. The analysis of the metrics such as CPU consumption, memory consumption, throughput, latency, MAE (Mean Absolute Error), RMSE (Root Mean Square Error), the usage of gas and the number of similar neighbors proves that *BC-SRDS* can significantly improve the accuracy and gain mor pro TI

II. LITERATURE SURVEY

Title-1: Elliptic Curve Cryptography Based Security Framework for Internet of Things (IoT) Enabled Smart Card

Authors: T. Daisy Premila Bai; K. Michael Raj; S. Albert Rabara

Description: Smart cards are adopted by people worldwide for different applications and they are only intra domain oriented due to security concerns. The literature study reveals that research has been carried out all over the world to strengthen the security requirements of the smart cards. But there is no research proposal to report that one smart card to support all application domains invariably. Hence, in this paper a novel Elliptic Curve Cryptography (ECC) based security framework for Internet of Things (IoT) enabled Smart Card is proposed. This is a secured and novel one for the public to access diversified smart applications with one Smart Card at anywhere and anytime. The security analysis ensures that ECC provides strong security for Smart Card implementation.

Title-2: Probabilistic Models for Unified Collaborative and Content-Based Recommendation in Sparse-Data Environments.

Authors: Alexandrin Popescul and Lyle H. Ungar, David M. Pennock and Steve Lawrence

Description: Recommender systems leverage product and community information to target products to consumers. Researchers have developed collaborative recommenders, content-based recommenders, and a few hybrid systems. We propose a unified probabilistic framework for merging collaborative and content-based recommendations. We extend Hofmann's (1999) aspect model to incorporate three-way co-occurrence data among users, items, and item content. The relative influence of collaboration data versus content data is not imposed as an exogenous parameter, but rather emerges naturally from the given data sources. However, global probabilistic models coupled with standard EM learning algorithms tend to drastically over fit in the sparse data situations typical of recommendation applications. We show that secondary content information can often be used to overcome sparsity. Experiments on data from the Research Index library of Computer Science publications show that appropriate mixture models incorporating secondary data produce significantly better quality

recommenders than -nearest neighbors (k-NN). Global probabilistic models also allow more general inferences than local methods like KNN.

Title-3: **BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT.**
Authors: Suhui Liu; Jiguo Yu; Yinhao Xiao; Zhiguo Wan; Shengling Wang; Biwei Yan
Description: The Internet of Things (IoT) changed our lives with huge amounts of data production. Due to source-limited IoT devices, one of the best ways to process the data is cloud storage. However, a series of security and privacy issues arise, such as illegal data access, data tampering, and privacy leak. Though symmetric encryption can guarantee data confidentiality, it cannot realize fine-grained data sharing and searching. The keyword-based searchable attribute-based encryption (KSABE) can achieve data confidentiality and fine-grained access control. More importantly, it realizes a keyword-based search for data users. However, the heavy decryption computation burden and the management of massive user keys appear when implementing attribute-based encryption schemes to IoT. Therefore, this article proposes a blockchain-aided searchable attribute-based encryption (BC-SABE) with efficient revocation and decryption, where the traditional centralized server is replaced with a decentralized blockchain system being in charge of the threshold parameter generation, key management, and user revocation. All revocation tasks are done by the blockchain and it is on longer necessary for ciphertext re encryption and key update.

Title-4: A Proposed Solution and Future Direction for Block chain-Based Heterogeneous Medicare Data in Cloud Environment
Authors: Harleen Kaur & M. Afshar Alam & Roshan Jameel & Ashish Kumar Mourya & Victor Chang
Description: The healthcare data is an important asset and rich source of healthcare intellect. Medical databases, if created properly, will be large, complex, heterogeneous and time varying. The main challenge nowadays is to store and process this data efficiently so that it can benefit humans. Heterogeneity in the healthcare sector in the form of medical data is also considered to be one of the biggest challenges for researchers. Sometimes, this data is referred to as large-scale data or big data. Block chain technology and the Cloud environment have proved their usability separately. Though these two technologies can be combined to enhance the exciting applications in healthcare industry. managing electronic medical records in a Cloud environment.

Title-5: Privacy-Aware Data Publishing and Integration for Collaborative Service Recommendation
Authors: Chao Yan; Xinchun Cui; Lianyong Qi; Xiaolong Xu; Xuyun Zhang
Description: Item-based collaborative filtering (i.e., ICF) technique has been widely recruited to make service recommendations in the big data environment. However, the ICF technique only performs well when the data for service recommendation decision-making are stored in a physically centralized manner, while they often fail to recommend appropriate services to a target user in the distributed environment where the involved multiple parties are reluctant to release their data to each other due to privacy concerns. Considering this drawback, we improve the traditional ICF approach by integrating the locality-sensitive hashing (LSH) technique, to realize secure and reliable data publishing.

Title-6: Secure Reviewing and Data Sharing in Scientific Collaboration: Leveraging Blockchain and Zero Trust Architecture
The current publishing landscape grapples with opacity in the review process. In response,
a proposal for a blockchain-driven system is put forth to establish transparent and auditable records for evaluations.
However, despite its decentralized nature, concerns persist regarding confidentiality and secure data sharing, crucial for fostering future collaborations. To address these challenges, this study advocates for the implementation of an access control mechanism (ACM) to safeguard confidentiality. Under this mechanism, only the assigned reviewer would have access to the confidential manuscript, ensuring the integrity of the review process. In scientific collaborations, the imperative for confidential datasharing extends beyond reproducibility to encompass vital collaborative endeavors such as publications,
Memorandums of Understanding (MoUs), grants, and funding.
While hierarchical ACM may prove
insufficient in defending confidential data, a more nuanced approach is proposed, leveraging a fine-grained access control model that considers contextual opinions, embodied in the concept of Zero Trust Architecture. Additionally, an incentivization mechanism based on author feedback is proposed to bolster reviewer
engagement and credibility.
In summary, this study aims to tackle trust and confidentiality concerns within
the review system, facilitating secure data sharing.

Title-7: privacy-aware data publishing and integration for collaboration service recommend
Authors: Chao yani, xinchun cui,lianyong qi1,2,xiaolong xu3 and xuyun zhang4
Description: Item-based collaborative filtering (i.e., ICF) technique has been widely recruited to make service recommendations in the big data environment. However, the ICF technique only performs well when
the data for service recommendation decision-making are stored in a physically centralized manner, while
they often fail to recommend appropriate services to a target user in the distributed environment where the
involved multiple parties are reluctant to release their data to each other due to privacy concerns. Considering
this drawback, we improve the traditional ICF approach by integrating the locality-sensitive hashing (LSH)
technique, to realize secure and reliable data publishing. Furthermore, through integrating the published data recommendation approach named ICFLSH. At last, simulated experiments are conducted on WS-DREAM data set. Experiment results show that ICFLSH performs better than the competitive approaches in terms of service recommendation accuracy, efficiency, and the capability of privacy-preservation
.

Title-8:Collaborative Filtering and Trust in Recommendations
Authors: Resnick, P., Iacovou, N., Suchak, M., et al. (1994). "GroupLens: An open architecture for collaborative filtering of netnews" – CSCW Conference
One of the earliest implementations of collaborative filtering (CF).
Relevance: Forms the foundation of modern CF-based recommendation systems.
**Massa, P., & Avesani, P. (2007). "Trust-aware recommender systems" – RecSys
Proposed integrating trust into collaborative filtering to improve robustness.
Insight: Blockchain can enhance trust modeling by recording verifiable user interactions.

Title-9:Hybrid Blockchain-Recommendation Frameworks
Authors: Singh, S., Jeong, Y.-S., & Park, J. H. (2020). "A decentralized privacy-preserving healthcare blockchain for IoT" – Sensors
Combined blockchain and ML for privacy-preserving medical recommendations.
Relevance: Shows that blockchain can support sensitive domain recommendations securely.

Alam, T., & Kanhere, S. S. (2022). "A Blockchain-based Reputation System for Decentralized Service Recommendation" – IEEE Blockchain
Built a reputation model using blockchain to rate and recommend services without a central authority.
Key takeaway: Reputation scores stored on-chain can increase the reliability of CF outputs.

Title.10: Federated Learning and Edge Computing in Recommendations
Authors: Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). "Federated machine learning: Concept and applications" – ACM TIST
Though not blockchain-specific, this is relevant for privacy-preserving recommendation.
Blockchain can enhance federated learning by verifying model updates and managing contributor incentives.

SYSTEM ANALYSIS

EXISTING SYSTEM

❖ Sarwar *et al.* [6] proposed a collaborative filtering algorithm based on items, which mainly calculates the similarity between items by analyzing the user's historical data. Because the number of users are much larger than the number of items, the computing of similarity between items is less sparse than that between users. Meanwhile, because the properties of items are fixed, we can calculate the similarity between items offline. Moreover, the calculation performance between items
is high. Compared with collaborative filtering algorithm based on users, the recommendation quality is greatly improved. However, the item-based collaborative filtering algorithm also brings new challenges: Firstly, the algorithm does not consider the difference between users, thus, the recommendation quality is poor; secondly, when a new item is added to the system, it is difficult to recommend the items that are similar to the new item to users, because it is not scored or there are few scores about the new item.

❖ In order to solve these problems, Jiang *et al.* [4] proposed a hybrid recommendation algorithm, which takes the advantages of the two algorithms that are item-based collaborative filtering algorithm and user-based collaborative filtering algorithm. They use the characteristics of attributes of users or items to obtain a better recommendation effect. However, the algorithm is based on specific applications and it is difficult to transplant and expand.

❖ Cheng *et al.* [7] proposed a method to improve the recommendation quality by introducing

metric learning into collaborative filtering algorithm. By measuring the distance between target user and candidate set, it separates the candidate set. And the items that have high similarity to user preference are close to the users while the items that have low similarity to user preference are far away from users, which reduces the influence of sparse data on the recommendation. Although the algorithm can alleviate the influence of sparsity on the recommendation, but it does not propose an effective method to deal with sparse data.

Proposed System

❖ To resolve these security issues many cryptography algorithms available. Cryptography can provide services, such as: integrity checking—reassuring the recipient of a message that the message has not been altered since it was generated by a legitimate source and authentication. Secure the cloud means secure the storage database hosted by the cloud provider. Security goals achieved by encryption/decryption process Encryption / Decryption process are combination of multiple algorithms.

❖ Our proposed work used the concept of Hash function along with several cryptographic tools to provide better security to the data stored on the cloud. A typical blockchain implementation might use a combination of these algorithms like SHA-256: Used to hash the entire block's data, ensuring that the data cannot be altered without changing the hash. ECC/ECDSA: Used to sign transactions (public/private keys) and ensure the authenticity of each transaction in the block. Merkle Trees are used to efficiently store and verify the integrity of all transactions in a block.

❖ Together, SHA-256, ECC/ECDSA, and Merkle Trees create a robust, secure, and efficient system for storing and verifying data in blockchain networks. They provide mechanisms for data integrity, authentication, and efficient verification, all of which are crucial for the decentralized nature of blockchain technology.

❖ The Advanced Encryption Standard (AES) is one of the most widely used encryption algorithms for securing data. It is a symmetric-key block cipher, which means the same key is used for both encryption and decryption blockchain framework for colloborative service .

III. METHODOLOGY

1. AES (Advanced Encryption Standard):

Purpose: AES is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption.

Importance: AES is widely regarded as one of the most secure and efficient encryption algorithms available. It works well with large datasets and is computationally efficient, which is essential for secure communication where performance is important. AES supports key sizes of 128, 192, and 256 bits, with AES-256 being the most secure. It's been extensively analyzed and is resistant to most types of attacks.

Use: In your system, AES can be used to encrypt the actual data being communicated, ensuring confidentiality during transmission

.

2. Elliptic Curve Cryptography (ECC):

Purpose: ECC is a public-key cryptography system that provides the same level of security as other public-key systems (like RSA) but with much smaller key sizes.

Importance: Efficient: ECC requires shorter keys to provide equivalent security levels. For example, a 256-bit key in ECC offers the same security as a 3072-bit key in RSA. This makes ECC more efficient in terms of computation and bandwidth usage. Scalability: ECC is highly suitable for mobile devices, IoT systems, and environments with limited computational resources.

Use: ECC can be used for secure key exchange, digital signatures, and public-key encryption in your system. It's particularly effective in the hybrid encryption scheme, where you encrypt data with AES and exchange the symmetric key using ECC.

3. SHA-256 (Secure Hash Algorithm 256-bit):

Purpose: SHA-256 is a cryptographic hash function that produces a fixed-size, unique output (256 bits) for any input data. It is a one-way function, meaning it is computationally infeasible to reverse the hash to retrieve the original input.

Importance: Integrity: It ensures that the data has not been tampered with during transmission. By generating a hash of the message and comparing it at the destination, you can verify whether the data has been altered.Collision Resistance: It's designed such that it is computationally infeasible to find two different inputs that produce the same hash (known as a "collision").

Use: SHA-256 can be used to hash messages and verify their integrity. In combination with a digital signature (e.g., ECDSA), it allows verification that the message hasn't been tampered with.

4. ECDSA (Elliptic Curve Digital Signature Algorithm):

Purpose: ECDSA is a variant of the Digital Signature Algorithm (DSA) that uses elliptic curve cryptography to create a digital signature for a message.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04609
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Importance: Authentication: ECDSA ensures that the message comes from a legitimate sender. It allows a user to sign a message with their private key, and others can verify this using the sender's public key. Efficiency: As with ECC, ECDSA provides strong security with smaller key sizes, making it more efficient than other digital signature algorithms like RSA
.
Use: In your system, ECDSA can be used to sign messages or verify the authenticity of messages and transactions. The combination of ECC and ECDSA ensures both secure key exchange and non-repudiation.

5. Merkle Trees:
Purpose: Merkle trees are a data structure that allows for efficient and secure verification of the integrity of large sets of data.
Importance: Efficient Verification: Merkle trees enable efficient verification of whether a piece of data belongs to a set, making it suitable for distributed systems like blockchain.Tamper Detection: Since each leaf node of a Merkle tree represents a hash of the data, and the internal nodes represent the hashes of their children, any modification to the data would require recalculating many hashes in the tree, which makes tampering detectable.
Use: In blockchain or distributed ledgers, Merkle trees are used to verify data integrity. In your project, they can be employed to securely store and verify the hash of messages or transactions on the blockchain, ensuring that any tampering is easily detectable.

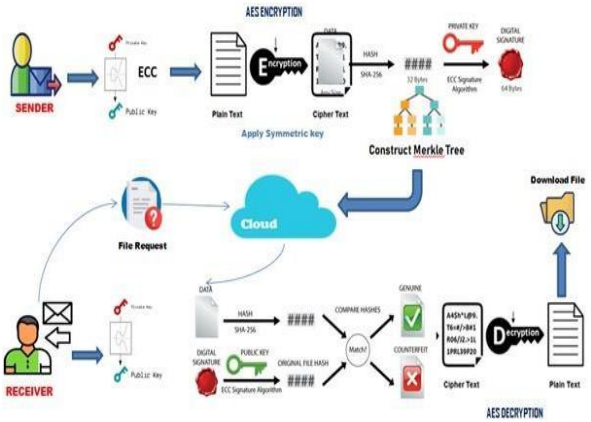
6. Hybrid Encryption: Use AES for message encryption (symmetric encryption) due to its speed and efficiency. Use ECC to securely exchange the AES key (asymmetric encryption) between the sender and receiver.

7. Message Authentication: Use SHA-256 to generate a hash of the encrypted message. Use ECDSA to sign this hash, ensuring the authenticity and integrity of the message.

8. Blockchain Integrity:
Use Merkle trees to organize and securely store the hash of the signed messages on the blockchain. This ensures that any tampering of the messages is easily detectable.

9. Collaborative Service Recommendation Scheme
AES ensures fast, efficient, and strong confidentiality of the data.
ECC provides a highly secure yet efficient way of managing key exchange and public-key cryptography.
SHA-256 ensures data integrity by generating a unique and fixed-size hash.
ECDSA guarantees authentication of the sender and ensures that the message hasn't been tampered with.
Merkle Trees provide a highly efficient way to verify the integrity of large data sets, making them perfect for blockchain applications.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION DETAILS

1. Data Owner Module
In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file's blocks and then store in the cloud. The data owner can check the replication of the file's blocks over Corresponding cloud server. The Data owner can have capable of manipulating View Files, Upload File, and Update File.

2. Cloud Server Module
The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data file's blocks and store them in the cloud for sharing with Remote User To access the shared data file's blocks, data consumers download encrypted data file's blocks of their interest from the cloud and then decrypt them and perform the following operations such as View Attackers, View Files, View Service Recommendations By Blockchain, Authorize User, Authorize Owner, Search Requests, Download Requests, View File Rank Results, View time Delay Results, view Through output Results.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04609
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

3. End User

In this module, remote user logs in by using his user name and password. After he will request for secrete key of required file's blocks from cloud servers, and get the secrete key. After getting secrete key he is trying to download file's blocks by entering file's blocks name and secrete key from cloud server and performs the following operations View Service Recommendations, Search, Download, View Files, Search Request, Download Request.

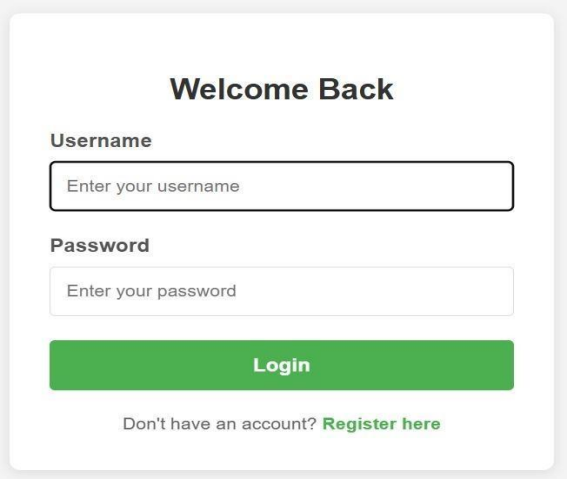
4. Data Encryption and Decryption

All the legal users in the system can freely query any interested encrypted and decrypted data. Upon receiving the data from the server, the user runs the decryption algorithm Decrypt to decrypt the cipher text by using its secret keys from different Users. Only the attributes the user possesses satisfy the access structure defined in the cipher text CT, the user can get the content key.

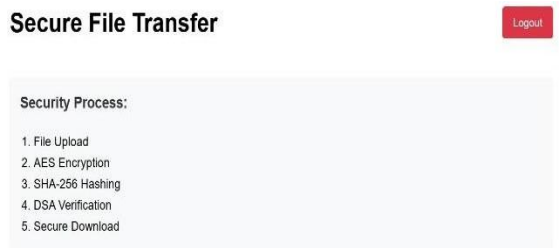
control actions will be used to generate a membership functions for a fuzzy set. Tuning is required during a construction of membership functions and rules. That is, it is necessary to measure a controller's performance and then alter a membership functions and rules accordingly. It will take lot of time to do this task. These four primary components make up a fundamental configuration of fuzzy logic control based systems, as seen in Figure 6.5: (I) fuzzy logic, (ii) knowledge base, (iii) inference engine, and (iv) defuzzification.

V RESULTS

Register Page

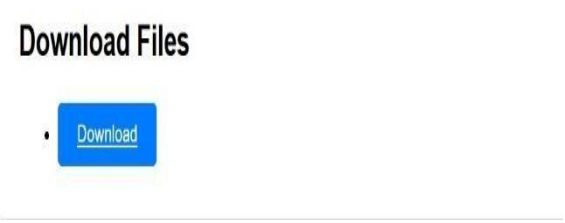


Login Page



File Transfer Page

Uploading File



Downloading File

V I CONCLUSION

he proposed system provides a highly secure method for data transmission by combining ECC, AES, and ECDSA techniques. ECC efficiently generates lightweight public-private key pairs suitable for modern networks. AES encryption ensures that the actual message remains confidential during transmission. ECDSA adds a layer of authenticity by digitally signing the message hash.

SHA-256 hashing and Merkle Trees enhance the integrity verification of the data. Blockchain integration strengthens the system by making stored data tamper-proof. The receiver can independently verify and decrypt the message with confidence. The implementation is lightweight, scalable, and secure. It suits cloud-based environments where data protection is critical. Overall, the project successfully meets the goals of secure, verifiable, and efficient message transmission.

REFERENCES

[1] A. Popescul, L. H. Ungar, D. M. Pennock, and S. Lawrence, ``Probabilistic models for uni_ed collaborative and content-based recommendation in sparse-data environments," 2013, *arXiv:1301.2303*. [Online]. Available: http://arxiv.org/abs/1301.2303

[2] G. Arora, A. Kumar, G. S. Devre, and A. Ghumare, ``Movie recommendation system based on users similarity," *Int. J. Comput. Sci. Mobile Comput.*, vol. 3, no. 4, pp. 765_770, 2014.

[3] J. Bobadilla, F. Ortega, and A. Hernando, ``A collaborative _ltering similarity measure based on singularities," *Inf. Process. Manage.*, vol. 48, no. 2, pp. 204_217, Mar. 2012. [4] C. Jiang, R. Duan, H. K. Jain, S. Liu, and K. Liang, ``Hybrid collaborativ _ltering for highinvolvement products: A solution to opinion sparsity and dynamics," *Decis. Support Syst.*, vol. 79, pp. 195_208, Nov. 2015.

[5] H. G. Rong, S. X. Huo, C. H. Hu, and J. X. Mo, ``User similarity-based collaborative _ltering recommendation algorithm," *J. Commun.*, vol. 35, no. 2, pp. 16_24, 2014.

[6] K.-Y. Chung, D. Lee, and K. J. Kim, ``Categorization for grouping associative items using data mining in item-based collaborative _ltering," *Multimedia Tools Appl.*, vol. 71, no. 2, pp. 889_904, Jul. 2014.

[7] C.-K. Hsieh, L. Yang, Y. Cui, T.-Y. Lin, S. Belongie, and D. Estrin, ``Collaborative metric learning," in *Proc. 26th Int. Conf. World Wide Web*, 2017, pp. 193_201.

[8] A. Mnih and R. R. Salakhutdinov,

``Probabilistic matrix factorization," in *Proc. Adv. Neural Inf. Process. Syst.*, 2008, pp. 1257_1264.

[9] C. Yu and L. Huang, ``A Web service QoS prediction approach based on time- and locationaware collaborative _ltering," *Service Oriented Comput. Appl.*, vol. 10, no. 2, pp. 135_149, Jun. 2016.

[10] X. Zhang, Z.Wang,W. Zhang, and F. Yang, ``A time-aware QoS prediction approach toWeb service recommendation," in *Proc. 4th Int. Conf. Comput. Eng. Netw.* Cham, Switzerland:

Springer, 2015, pp. 739_748.

[11] H. Li, ``Learning to rank for information retrieval and natural language processing," *Synth. Lect. Hum. Lang. Technol.*, vol. 4, no. 1, pp. 1_113, Apr. 2011.

[12] S. Badsha, X. Yi, I. Khalil, D. Liu, S. Nepal, E. Bertino, and K.-Y. Lam, ``Privacy preserving location-aware personalized Web service recommendations," *IEEE Trans. Services Comput.*, early access, May 22, 2018, doi:10.1109/TSC.2018.2839587.

[13] J. Zhu, P. He, Z. Zheng, and M. R. Lyu, ``A privacy-preserving QoS prediction framework for Web service recommendation," in *Proc. IEEE Int. Conf. Web Services*, Jun. 2015, pp. 241_248.

[14] T. R. Hoens, M. Blanton, A. Steele, and N.

V. Chawla, ``Reliable medical recommendation systems with patient privacy," *ACM Trans. Intell. Syst. Technol.*, vol. 4, no. 4, pp. 1_31, Sep. 2013.

[15] H. Polat and W. Du, ``Privacy-preserving collaborative _ltering using randomized perturbation techniques," in *Proc. 3rd IEEE Int.*