International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.48047/intjecse/v13i2.21224 ISSN: 1308-5581 Vol 13, Issue 02 2021

BLOCKCHAIN-ENABLED COLLABORATIVE SERVICE RECOMMENDATION SCHEME

[#1]KOKKULA SANJU,
[#2]DASARI VEENA,
[#3]B.RAMESH, *Assistant Professor,*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: The rapid growth of cloud computing has resulted in the spread of a wide range of online services. This complicates the process for users in determining which ones best meet their needs. Users require web service suggestions, which are only possible through the use of guided algorithms. Some of these algorithms have undergone further evaluation. Undoubtedly, a considerable number of present guiding systems rely on a jumble of old data, potentially revealing a weak point of entry. Cloud service providers frequently store sensitive diplomatic material that may jeopardize the privacy of their clients; as a result, these firms are typically hesitant to disclose such information. In addition to increasing revenue, providing secure data transmission between cloud platforms can become an important component of future recommendations targeted at overcoming the challenges we've already described. This paper provides a collaborative service suggestion system (BC-SRDS) that uses blockchain technology. We typically use ciphertext-policy attribute-based encryption (CP-ABE) to protect the data. This approach prioritizes data security and privacy. Following that, we looked at specific examples of negligence and planned attacks, such as Distributed Denial of Service (DDoS) and Denial of Service (DoS), that were carried out via data transmission via the blockchain. Furthermore, the blockchain ensures data security and immutability. A locality-sensitive hashing method is also used to ensure that customers may rely on our services. The security analysis shows that BC-SRDS successfully protects data privacy, prevents tampering, and ensures data integrity. Multiple reviews have shown that BC-SRDS produces better recommendations than competing techniques.
Keywords: Collaborative servicere commendation, blockchain,data distribution.

1. INTRODUCTION

Because of the constant improvements in computing and the Internet, a plethora of network information services have become essential components of people's daily lives. Users gain several advantages from these services. Despite this, the amount of information generated by Internet users continues to grow rapidly. The term for this is "information overload." Internet service providers face considerable problems in ensuring extensive product uptake and efficiently picking services based on user data. Internet users must devote significant effort and time combing through massive amounts of information in order to find the services that pique their interest. The assistant editor is assisting with this article's review.

Collaborative filtering recommendation is a popular algorithm that has proven to be effective in tackling these difficulties. It makes individualized suggestions to the intended audience based on the scoring records of available resources. Despite making great recommendations, the collaborative filtration selection system still has several flaws. The collaborative filtering recommendation algorithm's reliance on data maintained on a central server renders historical data ineffective as a reference for new users or items. As a result, the software may have cold starts and fail to complete all platforms. Nonetheless, there is a potential solution to the problem of chilly starts. B. Use case: User A called Amazon customer support, while User B contacted IBM. Customers A and B who are similar can use B's offerings to propose services to A or evaluate A's products to recommend services to B. Amazon and IBM are cautious about sharing user data in order to protect their customers' privacy. This drastically diminishes the value of the advise because it is impossible to identify new consumers who are similar to current users. The issue of cloud systems experiencing long online reaction times due to data dispersion across multiple remote platforms, resulting in significant transmission costs, remains unresolved.

In light of the aforementioned difficulties, this study suggests the deployment of a novel collaborative service recommendation system (BC-SRDS) based on blockchain technology and data sharing. This strategy secures data exchange between platforms by utilizing blockchain technology. Furthermore, locality-sensitive hashing (LSH) provides an effective and quick way to locate connected data, making it valuable for making instant recommendations. The following is a quick summary of the key input:

1. It is widely known that only a small number of recommendation algorithms use blockchain technology to generate suggestions. Despite the fact that a large number of these algorithms rely on collected data. User privacy concerns limit the ability of remote cloud services to collaborate on ideas by exchanging data. This study investigates the ability of blockchain technology to offer correct recommendations and create a secure platform for information

sharing.

2. Unlike most other approaches, our methodology combines CP-ABE (ciphertext-policy attribute-based encryption) with blockchain technology to facilitate data sharing between cloud platforms, protect the confidentiality of data provenance, reduce the likelihood of single point negligence, improve data integrity, and thwart DoS or DDoS attacks.
3. To demonstrate the efficacy of BC-SRDS, the experiment makes use of the WS-DREAM dataset, a valuable distributed dataset developed to assess quality of service (QoS). A wide range of parameters are assessed, including but not limited to CPU and memory usage, throughput, latency, root mean square error (RMSE), mean absolute error (MAE), gas consumption, and the number of comparable peers. The findings show that BC-SRDS has the potential to greatly improve revenue and accuracy.

2. RELATEDWORK

The three basic types of guided algorithms are content-based recommendation algorithms, joint filtering recommendation algorithms, and hybrid recommendation algorithms. Among them, the joint filtering algorithm, also known as the social filtering algorithm or the cooperative filtering algorithm, performs the best. It is widely used in the transport, governance, and education sectors. The original algorithm for collaborative filtering proposals prioritizes the user. It examines the target user's previous site usage and uses a specific algorithm to determine the level of similarity between the target user and other users with comparable characteristics. The software closes by recommending services to target consumers that have been used by similar users but not by the target users. In order to produce tailored recommendations. The user-based collaborative filtering suggestion algorithm faces a variety of obstacles as Internet user numbers and network capacities grow rapidly, including scalability, cold start, and sparsity issues. Sarwar et al. created an item-based joint filtering algorithm that assesses the degree of similarity between two things largely utilizing the user's history data. The similarity computation between items is denser than the similarity calculation between persons since there are more humans than objects. Furthermore, calculations using objects demonstrate a significantly high level of computing efficacy. When compared to the user-based joint filtering strategy, the recommendations improve significantly in quality. However, item-based collaborative filtering has the following extra drawbacks: Fundamentally, the algorithm fails to account for individual variances, producing less exact recommendations. Furthermore, the introduction of a new item into the system makes it harder for users to endorse similar things because there are no or a limited number of scores for the new item. Jiang et al. developed a hybrid suggestion algorithm to address these challenges, combining the most successful characteristics of the item-based and user-based collaborative filtering algorithms. The algorithm's reliance on certain applications makes it difficult to extend and relocate. Cheng et al. proposed combining metric learning into the joint filtering algorithm to improve the precision of recommendation. As part of the procedure, the candidates are split based on the distance between them and the target individual. Furthermore, it is important to note that products that closely fit with consumer preferences are placed close to users, but those that do not are kept at a significant distance from users. This reduces the impact of the inadequate data on the proposal. While the strategy may help to reduce the influence of sparsity on concepts, it is not a realistic way to deal with sparse data. Numerous people use the Mnih matrix decomposition approach, which is a well-known model-based collaborative filtering tool. When circumstances are sparse, the item-based collaborative filtering method performs better than the user-based collaborative filtering method. Yu et al. took into account the geographical situation.

They recognized a link between people who lived close together and frequently used the same service for similar needs. Furthermore, there is a strong association between time and the quality of internet service. As a result, it is advised that you use a time-based QoS modeling technique. Because user choices have a substantial impact on the quality of recommendations, and recommendations cannot be executed precisely at the appropriate moment or location. Li et al. increased the recommendation algorithm's fit to users' needs by including the user choice demand model with sorting learning technology.

Users are invited to submit further information to enhance the usability of proposals for web services. However, the obligation for managing the users' data remains with the service provider, hence raising the possibility of critical foreign information being compromised. In the case that merged systems are not appropriately controlled, confidential user information may become public. User information could still be compromised if unwanted nodes obtain access to the amalgamate server and seek to sell it to third parties. As a result, Badsha et al. proposed a mechanism for ensuring privacy that can approximate the nonexistent QoS value. In addition to assessing Quality of Service data, the user's location is a consideration in selecting which online services to deliver. The protocol encrypts location and quality of service (QoS) information for the user. This secures their privacy while enabling the protocol to present them with appropriate service recommendations. Zhu et al. deployed data obfuscation technology to guarantee secrecy by strengthening the original dataset with encoded data, so obscuring the genuine service quality data. Additionally, some persons have suggested protecting privacy via cryptography, randomization, and anonymization in addition to existing collaborative filtering techniques. Additionally, Zheng et al. built a privacy-preserving solution for Industrial Internet of Things data exchange. While utilizing blockchain technology for data sharing, Wang et al. neglected to evaluate the

security consequences of the given information. To promote data exchange, Liu et al. also developed a blockchain-assisted searchable attribute-based encryption for cloud-IoT. Furthermore, Cai et al. proposed a secure and efficient approach for data sharing.

3. SCHEMEOVERVIEW

OVERVIEW

This study presents a data-distributed collaborative service recommendation system based on blockchain technology. There is a more secure way to transport data than using the schemein. Instead, we use the CP-ABE protocol, which allows cloud platforms to retain control over their data while assuring secure data transfer. The data owners are responsible for managing user data because CP-ABE integrates the access strategy directly into the ciphertext. It also prohibits unauthorized parties from accessing the user's previously provided service information. Thus, the technique meets the security requirements for storing user previous service data. We also plan to disseminate information using blockchain. Cryptext is already quite safe, but anarchy and its inherent invulnerability can strengthen it even further. If there are any changes to the data, our method makes it easier to identify them. Therefore, expressing our plan is logical. Figure 1 also shows a simplified version of the system model for our approach. The design components are divided into three main categories: data, user, and data distribution.

1. User layer: The majority of these layers are made up of various privately owned devices that allow people to connect to the internet. They will generate a large volume of data on the cloud systems. Keep in mind that these consumers are spread over multiple channels.
2. Data distribution layer: Consensus across cloud systems on data sharing leads to the establishment of a consortium blockchain, allowing for message exchange. The consortium blockchain will serve as the repository for all shared information. Platforms can improve income by combining blockchain data with their own and leveraging the results to make more precise recommendations. Each platform cooperate to keep the record accessible.
3. Data layer: At this level, incredibly huge films and photographs are kept on cloud servers because blockchain technology is not intended to handle massive amounts of data.

Users initially seek a cloud platform that allows them to choose which services to use (Figure 1). Users not only send queries that are kept on cloud servers, but they also generate large amounts of data. It is reasonable for various cloud platforms to collaborate and share data in order to improve customer happiness and gain additional benefits. The goal is to create a decentralized consortium blockchain that connects all cloud services. A cloud platform transfers data to another cloud platform. Furthermore, their ability to retrieve communal data allows them to make exact recommendations. Customer service information is encrypted using CP-ABE before being sent to the blockchain. This may protect user privacy. Access to encrypted data is restricted to platforms that meet the stated attribute requirements. The protected data CT is then added to the blockchain under transaction I. After being uploaded to the consortium blockchain, the events are combined into a block that all nodes can verify and execute. A successful mining operation will result in the correct documentation of the transaction on the consortium blockchain. Despite the limits of blockchain technology, large media like videos and photos continue to be transferred to cloud servers. They can decrypt the shared data by receiving the encrypted data CT, assuming the cloud platform's features are properly established. Finally, the decrypted data will be combined with the cloud platform's data to give clients with exact suggestions.

SECURITYDEFINITION

1. SECURITYMODEL

Our proposed solution meets the criteria for data privacy, which is a fundamental component of security. Using the security exercise, we can demonstrate that our data is secure. The security model for the CP-ABE approach will now be discussed.

1. **Setup.** The procedure is executed by challenger C, who then delivers the public parameters and PK to adversary A.
2. **Phase1.**Adversary A conducts a series of iterative queries in an attempt to retrieve the private keys for the attribute set S1,...,Sq1.
3. **Challenge.** A transmits two messages of the same length, m0 and m1. A demands a stringent $A\prec$ access structure, ensuring that none of the attribute sets S1,...,Sq1 meet $A\prec$'s criteria. C randomly selects bit b, which is then used to encrypt the message mb with the $A\prec$ method. A person receives the decrypted text CT.
4. **Phase 2.** Phase 1 is repeated since none of the attributes assigned to Sq1+1,...,Sq meet the requirements of the access structure. This is well aligned with the existing assignment.
5. **Guess.**The probability, indicated as Pr, is the possibility that A will win this game.Theprobability$\Pr[b' = b] - \frac{1}{2}$ isdefinedasA'sadvantagetowinthis game.

Definition 1: A CP-ABE strategy is regarded secure if each of its adversaries, capable of solving problems in polynomial time, has a marginal advantage in the preceding game.

2. SECURITYPROPERTIES

We believe that every cloud platform that uses the group blockchain is "honest but inquisitive" and will refrain from exploiting or leaking program-related data. Each cloud platform is capable of utilizing shared information ethically. To ensure that the proposed solution works, the following important security precautions must be applied.

- **Tamper-proofing.**It is preferable for all nodes to preserve the shared data with minimal changes. After a node modifies data, it is possible to locate previously shared data.
- **Avoidingsinglepointofnegligence.**It is vital that the plan considers the requirement that other cloud platforms continue to operate regularly in the case of an assault on one.
- **DataHonesty.**The technique can quickly evaluate whether the data is at capacity for shared data manipulation.
- **DefendingagainstDoSorDDoSattacks.**DoS (Denial of Service) and DDoS (Distributed Denial of Service) assaults can be mitigated using this strategy, which blocks a huge number of requests from attackers. This ensures the system's regular operation.

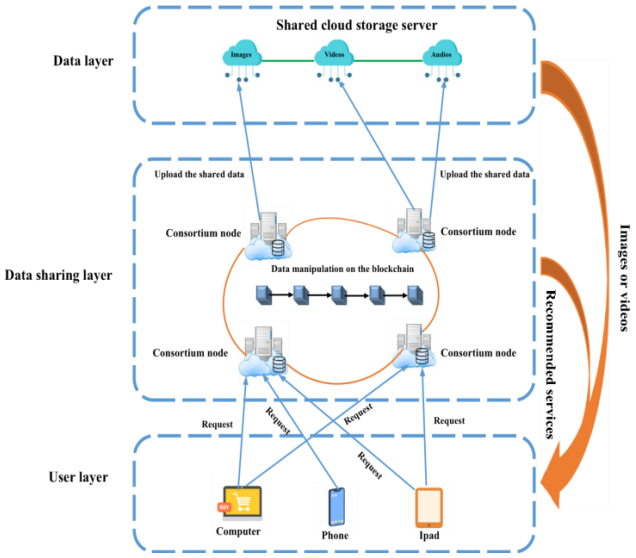

FIGURE1. The model of service recommendation using blockchain.

4. COLLABORATIVE SERVICERECOMMENDATION SCHEME

In accordance with the project structure, this part provides a detailed explanation of the system's construction. To help you understand, we'll start by providing a brief summary of the method. Our technique uses CP-ABE (Ciphertext-Policy Attribute-Based Encryption) to protect shared data and assure data provenance integrity. Furthermore, blockchain technology assures that only authorized individuals have access to sensitive information. Each node in the blockchain will have a unique copy of the shared data. This ensures data accuracy by reducing the possibility of a single point of failure. Decryption of shared data is currently limited to people who meet the access tree criteria. This is done to lessen the security risks associated with key transmission in typical symmetric key encryption while also protecting data privacy. Transferring data between cloud platforms via blockchain technology protects data quality, lowers communication costs, and increases service concept correctness. The original locality-diplomatic strategy is used to achieve concord. This improves the user experience while also expediting the matching process. Table 1 defines the markers.

TABLE 1. Notations.

Symbol	Semantics
u	the number of users in each cloud platform
I_j	the j-th service
$I_{i,j}^q$	the j-th quality dimension q of I_j in platform cp_i
l	the number of the hash functions
cp_i	the i-th cloud platform
N_c	the number of cloud platforms
n	the number of web services
L	the number of hash tables
$\mathbb{G}_0$	$\mathbb{G}_0$ is a multiplicative cyclic group
p	p is the prime order of $\mathbb{G}_0$
λ	the security parameter of the system
t	the t-th hash table
g_1	the generator of $\mathbb{G}_0$
g_2	it is an element in $\mathbb{G}_0$
MSK	it is the master secret key
PK	it is the public key
SK	it is the private key
$\mathcal{T}$	a tree access structure
x	x is a node in $\mathcal{T}$
j	an attribute belonged to the user
S	a set of attributes
CT	the ciphertext of plaintext m

ALGORITHM DEFINITION

The suggested method consists basically of seven algorithms: construct, KenGen, distribute data, decode, and configure indexes for individual services. Combining offline indexes with service ideas produces the most effective service index.

1. **Setup.** The smart contract generates the master key and public key, represented by λ.
2. **KenGen.**The key generating facility carries out the key manufacturing process. When the system receives the S attributes of one cloud platform, it generates a unique key that can be used to locate the S attributes of another cloud platform.
3. **ShareData.**The cloud platform runs the method after receiving the data m, the public key PK, and the access structure T. The program is now creating a ciphertext CT for the group blockchain.
4. **Decrypt.** The cloud platform receives the ciphertext CT, public key PK, and private key SK and then executes the method. The technique turns ciphertext CT into plaintext m.
5. **Build indices for each service.** The cloud computing platform governs Alphabet's execution. The software accepts any type of input and returns web service IDs as an output.
6. **Get the final service index by integrating indexesoffline.** The sub-index of online services is sent to the cloud platform. The "I" in the web-based service symbolizes the input and the service index, which is the ultimate output.
7. **Servicerecommendation.**The computer collects information about the service desired by the target user and then provides recommendations for them based on similar services.

5. CONCLUSION

This article looks at the architecture of the BC-SRDS service recommendation system. It makes precise service suggestions to clients and facilitates data interchange between platforms via the consortium blockchain. To protect data security, it is encrypted via the CP-ABE method before being transmitted to other cloud platforms. Blockchain technology lowers the possibility of Denial of Service (DoS), Distributed Denial of Service (DDoS), and single point of failure attacks on cloud services. Furthermore, it gives customers rapid access to shared information, which may be used to earn additional cash. According to the security analysis, BC-SRDS is successful at preventing interference, preserving data integrity, and maintaining information confidentiality. Finally, we assess the efficacy of our strategy by running many tests with WS-DREAM. Experiment findings show that BC-SRDS is more accurate than the other three approaches. In addition, fuel costs for cloud computing systems are cheap. Furthermore, the effectiveness of our consortium's blockchain-based strategy may be evaluated using measures such as latency, throughput, and resource usage.

REFERENCES

1. Popescul,L.H.Ungar,D.M.Pennock,andS.Lawrence, ‘‘Probabilistic models for unified collaborativeandcontent-basedrecommendationinsparse-dataenvironments,’’2013,*arXiv:1301.2303*.[Online].Available:http://arxiv.org/abs/1301.2303
2. G.Arora,A.Kumar,G.S.Devre,andA.Ghumare,‘‘MovieRecommendationsystembasedonuserssimilarity’’*Int.J. Comput.Sci.MobileComput.*,vol.3,no.4,pp.765–770,2014.
3. J.Bobadilla,F.Ortega,andA.Hernando,‘‘Acollaborative filteringSimilaritymeasurebasedonsingularities,’’*Inf.Process.Manage.*,vol.48,no.2,pp.204–

217,Mar.2012.

4. Jiang,R.Duan,H.K.Jain,S.Liu,andK.Liang,''Hybridcollaborativefilteringforhigh-involvementproducts: 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, ''Usersimilarity-basedcollaborativefilteringrecommendationalgorithm,''*J. Commun.*, vol.35, no. 2, pp.16–24,2014.
6. K.-Y. Chung, D. Lee, and K. J. Kim, ''Categorization forgroupingassociativeitemsusingdatamininginitem-basedcollaborativefiltering,''*MultimediaToolsAppl.*,vol.71,no.2,pp.889–904,Jul.2014.
7. C.-K.Hsieh,L.Yang,Y.Cui,T.-Y.Lin,S.Belongie,andD. Estrin, ''Collaborative metric learning,'' in *Proc. 26thInt.Conf.WorldWide Web*,2017,pp.193–201.
8. Mnih and R. R. Salakhutdinov, ''Probabilistic matrixfactorization,'' in *Proc. Adv. Neural Inf. Process. Syst.*,2008,pp.1257–1264.
9. Yu and L. Huang, ''A Web service QoS predictionapproach based on time- and location-aware collaborativefiltering,'' *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-awareQoSpredictionapproachtoWebservicerecommendation,'' in*Proc. 4th Int. Conf. Comput. Eng.Netw.*Cham, Switzerland: Springer, 2015,pp. 739–748.