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

Real-Time User-Service Centric Historical Trust Model Based Access Restriction in Collaborative Systems with Blockchain Public Auditing in Cloud

Mr.N. Vel Murugesh Kumar[1], Dr. D. Naveen Raju[2], Dr. Gopirajan PV[3], Dr.P.Subhashini[4]

Submitted: 18/10/2022 **Revised:** 21/12/2022 **Accepted**: 19/01/2023

Abstract: The recent collaborative systems works over the cloud environment which is being encouraged by various service providers in reality. The organizations maintain numerous data in cloud which has been accessed and shared by various users of the environment. The service provider has the responsibility in maintaining the originality of the data and maintaining the security of the data. To enforce both of them, various access restriction and public auditing schemes are available. Number of approaches uses different features of user as well as service. However they suffer to achieve expected performance in data security and public auditing. To handle this issue, a novel real-time User-Service Centric Historical Trust Model with Blockchain Public Auditing (USHTM-BPA) is presented in this article. The method computes User Centric Trust Score (UCTS) and Computes Service Centric Trust Score (SCTS) to measure Trust Weight for the user towards secure access restriction. Further, the method adapts Feature Level Blockchain Public Auditing (FLBPA) which measures feature centric trusted access score (FCTAS) in restricting illegal access to improve data security in public auditing. The proposed method improves the performance of public auditing in collaborative systems and improves data security in cloud.

Keywords*:* *Cloud System, Collaborative Systems, Data Security, Access Restriction, Public Auditing, USHTM-BPA, UCTS, SCTS, FLBPA*

1. Introduction

The increased use of service orient environment increases the issues in data security. As the most organizations maintains their data in cloud which is intended to provide services to various users of the organization which can be accessed in a collaborative way, it introduces different challenges in various factors. Presence of data in collaborative environment allows the users of the system located in different geographic location to access the data to perform their task given. In this case, the data faces different challenges in terms of security as the presence of illegal user introduces security threats. For example, the user who is present in the environment would try to access the data to which the user has not access. This malicious access would leads to data stealing and would affect the performance of the entire system.

The presence of malicious access can be override by enforcing different access restriction schemes. The access restriction in cloud has been enforced with profile based, key based, feature based and service based approaches. In case of profile based approach, the method allows the user to access the data only when there is access mentioned in the data profile, similarly the key based approach verifies the given key for the grant of access. On the other side, the feature based approach verifies the grant available for each feature in the data to allow access to the user. In case of service based approach, the user has been verified for the access for the service. In all the cases, the adversary is capable of overriding the system and capable of accessing the data illegal way. This really affects the security performance of the model and affects the performance of entire cloud.

The other form of security issue is maintaining the originality of the data. The data stored and accessed from the cloud must be original when the data has been accessed by multiple users in the collaborative system. The cloud service provider has the responsibility in maintaining the originality of the data. It has been enforced by enforcing efficient public auditing schemes. There are number of public auditing schemes available which checks the data given for its originality in block level. However they suffer to achieve higher performance in public auditing. To

[1]Department of Computer Science and Engineering, R.M.K. Engineering College, Kavaraipettai-601206, Gummidipoondi Tk, Thiruvallur Dist., Tamil Nadu,India.
[2] Department of Computer Science and Engineering, R.M.K. Engineering College, Kavaraipettai-601206, Gummidipoondi Tk, Thiruvallur Dist., Tamil Nadu,India.
[3]Department of Computational Intelligence, SRM institute of science and technology, Kattankulathur campus.
[4]Department of Information Technology, Vel Tech Multi Tech dr.rangarajan dr.sakunthala engineering college, Chennai.
Corresponding Author Email : [1]murugobi@gmail.com, [2]drnaveenraju@gmail.com, [3]gopivrajan@gmail.com, [4]subhasaash@gmail.com

support this data security, blockchain techniques are greatly used in recent times.

Blockchain is the most recent technique in data sharing which restrict the malicious users in accessing the blocks of data in the chain. The user can access only when they are allowed and they should know how to decrypt the data with specific key and schemes should be identified from the hash code part of the block. This technique has been adapted to the public auditing and data security with different schemes. This paper describes such a novel approach in improving data security as well as public auditing in collaborative systems. The USHTM-BPA model focused on restricting the malicious access according to the historical behavior of the user at different levels. Also, the method uses block chain to share data between the users and computes UCTS (User Centric Trust Score) , SCTS (Service Centric Trust Score), and FLBPA (Feature Level Blockchain Public Auditing). The detailed approach is discussed in the next section.

2. Related Works

There exist numerous techniques available and discussed by researchers around the problem. This section details some of the methods related to collaborative systems and data security in cloud.

In [1], a secure and authenticated data storage, access, and sharing model is proposed for private cloud storage, which provides the user with secure storage of information. The data-sharing component enables sharing the stored data under the control of the data owner. The data access component enables authenticated access to the cloud storage.

An smart contract based approach is presented in [2], which integrates off-chain storage systems including cloud storage with Interplanetary File System (IPFS). The registered participants are provided with access privileges based on their roles to ensure that restrictions are enforced on-chain. Smart contracts are developed to maintain data provenance and generate reliable alerts and notifications.

In [3], a public auditing scheme is presented which provides faster magnitude by using auditing challenge-response protocol which in turn reduces the verification speed.

In [4], a collaborative public auditing framework is presented which uses auditing delegations and record them permanently, thereby preventing entities from deceiving each other. In [5],   a certificate less multi-replica and multi-cloud data public audit scheme based on blockchain technology is presented. The method uses dynamic hash table and modification record table which update group user data and identity tracking. All replicas are stored in different cloud servers, and their integrity can be audited at the same time.

A novel storage auditing scheme is presented in [6], which is capable of achieving user revocation independent of the total number of file blocks possessed by the revoked user in the cloud. A consortium based block chain distributed secure search (CBDSS) is discussed in [7], which is designed to perform secure communication in E-commerce system with blockchains.

A concurrent Practical Byzantine Fault Tolerance (PBFT) consensus method C-PBFT is presented in [8], which handles inefficiency of consensus due to fast node expansion. Similarly, an intelligent mediator-based enhanced smart contract is presented to protect sensitive data and uses block chain to manage private information [9].

A block chain based trusted routing scheme is presented in [10], which uses reinforcement learning towards improving the security in routing. The route a node on the chain collects the routes using chain and based on that routing is performed. To identify the malicious nodes in WSN, a block chain trust model (BTM) is presented in [11], which construct the chain to detect malicious nodes in a 3D space with the smart contract available.

A distributed collocation storage system with block chain security is presented in [12] to support WSN which uses asymmetric signature to enforce security. The security in data retrieval system is enforced in [13], which extract the cipher text which is indexed using porter stemming algorithm. The method uses the blowfish data encryption and ECC to support data security. Similarly, a proxy re-encryption algorithm is prescribed in [14], which is combined with erasure code to perform secure storage and retrieval. Similarly, a sliced revocable solution named RS-CPABE is presented in [15], which uses AES to perform re-encryption to improve data security.

In [16], a multi attribute trust model with fuzzy logic (MATM-FL) is presented which measure the trust according to the fairness, success rate, elapsed time and correctness of data. Using all these values, the fuzzy logic is enforced to measure the trust of nodes. Because of different features considered are in numeric form and they also comes on different values. By considering the range values in form of fuzzy logic, the trust of any user can be measured to enforce data security and access restriction.

All the above discussed approaches suffer to achieve higher performance in data security and public auditing.

3. Real-Time User-Service Centric Historical Trust Based Access Restriction and FLBPA Public Auditing Model

The proposed user service centric historical trust based access restriction and feature level blockchain public auditing (USHTM-FLBPA) maintain the traces of service access made by different users in the environment. The method receives the user request and enforces User-service Centric Historic Trust Access Restriction scheme to restrict malicious access from the illegal user. Further, the method perform feature level block chain public auditing to enable public auditing on the data given where the block chain has been generated according to the service data using Feature Centric Block Chain Generation (FCBCG) scheme. The detailed approach is presented in this section.

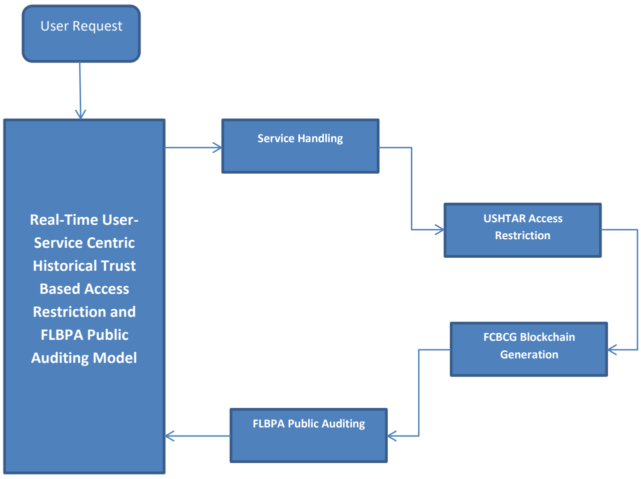
User Request
Real-Time User-Service Centric Historical Trust Based Access Restriction and FLBPA Public Auditing Model
Service Handling
USHTAR Access Restriction
FCBCG Blockchain Generation
FLBPA Public Auditing

Fig. 1: Architecture of Proposed USHTAR-FLBPA Model

The functional architecture of proposed model is presented in Figure 1, which has number of functional components and explained in detail in this section.

3.1 Service Handling

The service handling algorithm receives the user request and performs access restriction with USHTAR Access Restriction and generates blockchain. Also, the method enforces the public auditing with feature level blockchain public auditing model. The method receives the result of both access restriction and public auditing to handle the access grant and restriction.

```
Algorithm:
Given: User request Ureq, Access trace AT
Obtain: Null
Start
    Receive user request Ureq, AT.
    Boolean b = perform USHTAR access restriction (Ureq, AT)
    If true then
        If access request then
            Grant access.
            Service data SD = service access result.
            Blockchain bc = perform FCBCG Block   Chain Generation.
            Send to user.
        Else if update request then
            Boolean c = perform FLBPA(Service data)
            If true then
                Perform data update.
            End
        End
    End
Stop
```

The above discussed algorithm receives the user request and handles the request in various steps according to access restriction and blockchain public auditing.

3.2 USHTAR Access Restriction

The access restriction in this model is enforced in two ways: one by user centric manner by computing User Centric Trust Score (UCTS) which shows the trust of the user in accessing various services in their history. It has been measured by computing the number of times the user has accessed different services and number of times the user has completed the access correctly. Second, the trust of user is measured against specific service being accessed in his/her history. It is performed by measuring Service Centric Trust Score (SCTS), which is being measured by computing the number of service access and number of completion. Using both of them, the method computes the value of Access Clearance Score (ACS) based on which the service access has been granted or denied for the user.

```
Algorithm:
Given: Access Trace AT, User Request Ureq
Obtain: Boolean
Start
    Read AT and Ureq.
    User U= User$\in Ureq$
    Service S = Service $\in Ureq$
```

```
        User Trace UT = $\sum_{i=1}^{Size(AT)} AT(i).User == U$

        Service Trace ST = $\sum_{i=1}^{Size(AT)} AT(i).Service == S \,\&\&\, User == U$

        Compute UCTS = $\frac{\sum_{i=1}^{size(UT)} UT(i).State==Complete}{Size(UT)}$

        Compute SCTS = $\frac{\sum_{i=1}^{size(ST)} ST(i).State==Complete}{Size(ST)}$

        Compute ACS = $\frac{SCTS}{UCTS}$

        If ACS>Th then
                Grant access
        Else
                Deny access
        End
Stop
```

The above discussed estimates UCTS and SCTS values according to the behavior of the user in access the service in historic. Based on that the method computes the value of ACS and based on that the access restriction is performed.

3.3 FCBCG Block Chain Generation

The service data generated by accessing the service has been used to produce the blockchain. The method reads the service data and counts the number of features in the service result. Accordingly, a block chain will be generated with K number of blocks and the service features are encrypted by choosing a random scheme for the feature from the scheme set available. Using the index of the scheme selected, the method applying index manipulation model which subtracts the index from size of scheme set and reverse the same over the size of key set. These details of index and result of manipulation are used to produce hash code for the feature selected. Similarly, for each block or feature, the method performs the same to encode and decode the original text. The block chain generated has been shared between the users to enforce security.

```
Algorithm:
Given: Service Data SD, Scheme set Ss, Key set Ks
Obtain: Blockchain B
Start
        Read SD, Ss, Ks.
        Feature list Fl = $\sum Features \in SD$
        Generate blockchain B = $\sum_{i=1}^{size(Fl)} CreateBlock(i)$ and Add to chain
        For each block b
                Random r = Math.rand(size(ss))
                Scheme index Hi = size(ss)-r.

                Key Index Ki = size(ks)-r.
                Scheme s = ss(Hi)
                Key k = ks(ki)
                Data d = Encrypt (f,s,k)
                b.data = d.
                b.hashcode = Hi+”@”+ki
        End
Stop
```

The above discussed algorithm represents how the block chain is generated with the data given. Generated block chain has been given to the user who can decrypt the data by performing reverse operation.

3.4 FLBPA Public Auditing

The feature level blockchain public auditing approach receives the data from the user. Once the data is received, the method identifies the set of features and their values from the chain. Now, the method selects a subset of users who are authorized to give acceptance for any update. It has been performed by choosing a set of authorizers from the profile given and gives the data to the authorizers. Based on the authorization result obtained, the method computes the value of Feature Level Audit Support (FLAS) from different authorizers. Finally, a cumulative update support (CUS) is measured and based on that the user has been allowed to perform update action on the data.

```
Algorithm:
Given: Service Data SD, Profile P
Obtain: Boolean
Start
        Read SD and P.
        Feature list Fl = $\sum Features \in SD$
        For each feature f
        Authorizer set Aus = $\sum_{i=1}^{size(P)} Random(1, size(P))$
```

```
                    For each authorizer a
                              Send the data to authorizer.
                              Audit merit Am = Receive reply from authorizer.
                    End
                    Compute FLAS = $\frac{\sum Am\rightarrow +ve}{size(Aus)}$
          End
     Compute cumulative update support CUs = $\frac{\overset{size(Fl)}{\underset{i=1}{Count(Fl(i).FLAS>Th)}}}{size(Fl)}$
          If CUS>Th then
                    Return true
          Else
                    Return false.
          End
Stop
```

The above discussed algorithm represents the working of public auditing and the method computes cumulative update support for the request according to the originality of the feature value given. Based on the value of CUS, the method decides the grant of update in the original data to maintain public auditing.

4. Results and Discussion

The proposed Real-Time User-Service Centric Historical Trust Based Access Restriction and FLBPA Public Auditing Model has been implemented and evaluated for its performance under various constraints. The results obtained have been compared with the result of various other models.

Table 1 Details of Evaluation

Parameter	Value
Tool	Microsoft Azure
Programming	Advanced Java
Number of Services	300

The metrics and details used for the performance evaluation is presented in Table 1. Accordingly, the method are measured for their performance under various metrics and compared in this section.

Table 2 Content Sharing Efficiency

	Content Sharing Efficiency		
	100 Services	200 Services	300 Services
CBDSS	75	82	85
BTM	81	86	88
PBFT	84	88	90
MATM-FL	86	90	93
USHTM-FLBPA	89	94	98

The performance of methods in content sharing efficiency is measured and compared in Table 2, where the proposed USHTM-FLBPA has produced higher content sharing efficiency than other approaches.

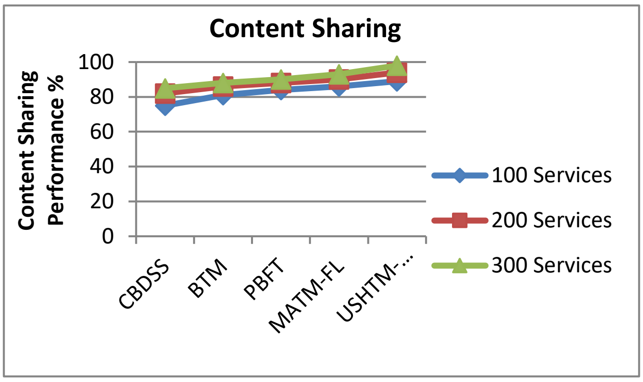

Fig. 2 Performance on content Sharing

The performance of various approaches in content sharing has been recorded and compared in Figure 2, where the proposed USHTM-FLBPA has achieved higher performance than other approaches.

Table 3 Analysis on Access restriction

	Performance on Access Restriction		
	100 Services	200 Services	300 Services
CBDSS	70	74	78
BTM	73	76	81
PBFT	75	81	84
MATM-FL	78	84	88
USHTM-FLBPA	85	88	97

The methods are measured for their access restriction performance and compared in Table 3. The proposed USHTM-FLBPA approach has produced higher performance in access restriction.

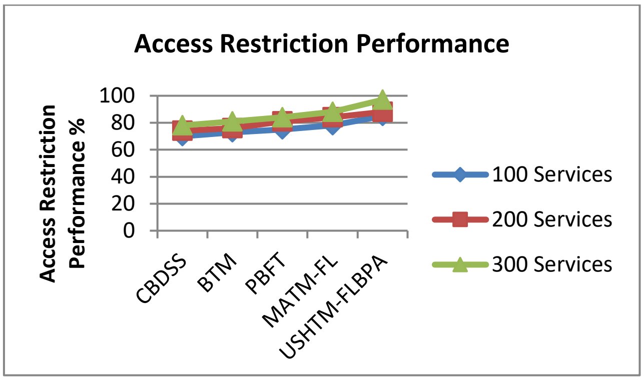

Fig. 3: Analysis on access restriction performance

The access restriction performance produced by USHTM-FLBPA model has been measured and compared in Figure 3. The proposed USHTM-FLBPA approach has produced higher access restriction performance than others.

Table 4: Analysis on Public Auditing Performance

	Performance on Public Auditing		
	100 Services	**200 Services**	**300 Services**
CBDSS	67	72	75
BTM	72	75	79
PBFT	76	79	82
MATM-FL	82	86	88
USHTM-FLBPA	85	89	97

The performance on public auditing has been measured and presented in Table 4. The proposed USHTM-FLBPA method improves the performance in public auditing up to 97% which is higher than any other approach.

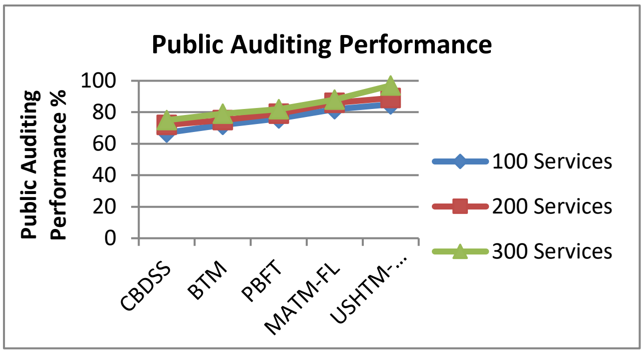

Fig. 4. Analysis on public auditing performance

The performance of USHTM-FLBPA towards public auditing has been measured on varying number of services. The proposed USHTM-FLBPA approach has produced higher public auditing performance than other approaches.

5. Conclusion

This article presented a user service centric historical trust based access restriction and feature level blockchain public auditing (USHTM-FLBPA) maintain the traces of service access made by different users in the environment. The method receives the user request and enforces User-service Centric Historic Trust Access Restriction scheme to restrict malicious access from the illegal user. Further, the method perform feature level block chain public auditing to enable public auditing on the data given where the block chain has been generated according to the service data using Feature Centric Block Chain Generation (FCBCG) scheme. The proposed approach improves the performance in access restriction, public auditing in collaborative environment.

References:

[1] H. Amintoosi et al., "Secure and Authenticated Data Access and Sharing Model for Smart Wearable Systems," in IEEE Internet of Things Journal, vol. 9, no. 7, pp. 5368-5379, 1 April1, 2022, doi: 10.1109/JIOT.2021.3109274.

[2] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar and S. Ellahham, "Blockchain-Enabled Telehealth Services Using Smart Contracts," in IEEE Access, vol. 9, pp. 151944-151959, 2021, doi: 10.1109/ACCESS.2021.3126025.

[3] C. Hahn, H. Kwon, D. Kim and J. Hur, "Enabling Fast Public Auditing and Data Dynamics in Cloud Services," in IEEE Transactions on Services Computing, vol. 15, no. 4, pp. 2047-2059, 1 July-Aug. 2022, doi: 10.1109/TSC.2020.3030947.

[4] P. Huang, K. Fan, H. Yang, K. Zhang, H. Li and Y. Yang, "A Collaborative Auditing Blockchain for Trustworthy Data Integrity in Cloud Storage System," in IEEE Access, vol. 8, pp. 94780-94794, 2020, doi: 10.1109/ACCESS.2020.2993606.

[5] X. Yang, X. Pei, M. Wang, T. Li and C. Wang, "Multi-Replica and Multi-Cloud Data Public Audit Scheme Based on Blockchain," in IEEE Access, vol. 8, pp. 144809-144822, 2020, doi: 10.1109/ACCESS.2020.3014510.

[6] Y. Zhang, J. Yu, R. Hao, C. Wang and K. Ren, "Enabling Efficient User Revocation in Identity-Based Cloud Storage Auditing for Shared Big Data," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 3, pp. 608-619, 1 May-June 2020, doi: 10.1109/TDSC.2018.2829880.

[7] Zhitao Guan, Achieving Secure Search over Encrypted Data for e-Commerce: A Blockchain Approach, ACM Transactions on Internet TechnologyVol. 21, No. 1, 2021.

[8] Xiaolong Xu, Concurrent Practical Byzantine Fault Tolerance for Integration of Blockchain and Supply Chain, ACM Transactions on Internet TechnologyVol. 21, No. 1, 2021.

[9] Juhno Kim, Intelligent Mediator-based Enhanced Smart Contract for Privacy Protection, ACM Transactions on Internet Technology Volume 21Issue 1February 2021 .

[10] Jidian Yang et al., “A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks”, Sensors, Vol.19, pp.1-19, 2019.

[11] Wei She, Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks, Research Gate, 2019.

[12] Qi Liu, Research on trust mechanism of cooperation innovation with big data processing based on blockchain, Springer Link (WCN), 2019.

[13] Chen Y, A Blockchain-Based Collocation Storage Architecture for Data Security Process Platform of WSN, IEEE (CSCWD), 2018.

[14] S. Mudepalli, et. Al "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing," IEEE (ICICCS), pp. 267-271, 2017.

[15] R. Nivedhaa and J. J. Justus, "A Secure Erasure Cloud Storage System Using advanced Encryption Standard Algorithm and Proxy Re-Encryption," IEEE (ICCSP), pp. 0755-0759, 2018.

[16] M. Bouchaala, et.al "Revocable Sliced CipherText Policy Attribute Based Encryption Scheme in Cloud Computing," IEEE (IWCMC), pp. 1860-1865, 2019.

[17] V. R. Prabha and P. Latha, "Fuzzy trust protocol for malicious node detection in wireless sensor networks", Wireless Pers. Commun., vol. 94, no. 4, pp. 2549-2559, 2017.