Taylor & Francis
Taylor & Francis Group

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

Trust aware cryptographic role based access control scheme for secure cloud data storage

K. Roslin Dayana & P. Shobha Rani

To cite this article: K. Roslin Dayana & P. Shobha Rani (2023) Trust aware cryptographic role based access control scheme for secure cloud data storage, Automatika, 64:4, 1072-1079, DOI: 10.1080/00051144.2023.2243144

To link to this article: https://doi.org/10.1080/00051144.2023.2243144

Published online: 15 Aug 2023.

AUTOMATIKA
2023, VOL. 64, NO. 4, 1072–1079
https://doi.org/10.1080/00051144.2023.2243144

Trust aware cryptographic role based access control scheme for secure cloud data storage

K. Roslin Dayana and P. Shobha Rani

Department of Computer Science and Engineering, R.M.D. Engineering College, Thiruvallur, India

ABSTRACT

Cloud data storage lets customers store vast amounts of data cheaply on demand. Cryptographic role-based access control (RBAC) systems preserve cloud data privacy by restricting access to users. This study develops a trust model to reason about and improve data security in cryptographic RBAC cloud storage systems. The trust degrees of the user determine the access rights to the data and are performed by User Activity Monitoring Agent (UAMA). Two different misconducts of users such as access policy violation and data leakage affect the trust degree of the user, which in turn upgrades the access policy. In addition, the user has to decrypt the data for gaining information from it, which is a second line of security. The performance of trust based RBAC scheme is evaluated with respect to different parameters such as illegitimate user detection, memory consumption, data storage with retrieval time and the proposed work performs better.

ARTICLE HISTORY
Received 20 June 2023
Accepted 26 July 2023

KEYWORDS
Secure cloud data storage; RBAC; cryptography; trust; data access

1. Introduction

Cloud computing provides its users with a broad range of services, while reducing user storage and computation with enhanced convenience of use [1,2]. As a result, it is witnessed that an increasing number of enterprises and individuals opt to store their data in the cloud. However, as a result of the expansion in scale and intensification of cloud computing, there has also been a progressive growth in study on fog and edge computing models. Concerns over data protection in the cloud have emerged as one of the most significant obstacles to the expansion of cloud computing [3–5].

Access control is one of the core technologies of cloud security, and it was one of the major cloud computing security focus topics. In the meantime, access control is also a major focus of research at the moment. The objective is to implement access control in order to prevent unauthorized users from accessing or stealing resources that have been stored in the cloud. Access control is an essential component of cloud computing, since the resources require the protection of relevant resources by means of access control [6].

The traditional computing model has undergone numerous modifications, while the processing and storage mode of cloud computing has seen many changes as well. These changes are mostly reflected in the following elements of cloud computing, such as the resources are not under the control of the users, trust is missing between the user and cloud, adaptable environment and virtualization concepts.

As a result of these issues, a significant amount of research in cloud access control has emerged at academic institutions and in the business world, and both sectors have attempted to implement already existing access control solutions [7–12]. However, each of them provides centralized storage and management modalities for identity information, as well as key, authority, authentication and other information. Therefore, the technology of access control still has two problems to solve in terms of privacy and security:

(1) An outside adversary launches an assault on the trusted centre, makes unauthorized changes to the database of authorized users that is kept on the central server, and gains unauthorized access to or steals the resources that users have stored in the cloud.
(2) A malicious cloud System Administrator (SA) may use the privilege to illegally access resources or tamper with the authorization database to do so.

Taking account of these considerations, this article tends to present a Role Based Access Control (RBAC) system, which offers data access patterns with respect to the role of the user. As pointed out above, data access by considering the roles of individuals may be misused and hence, the proposed work in this paper places two checkmates of security. Here, the data access permissions are strictly on the basis of roles and the stored data is encrypted, such that the user has to decrypt it before

CONTACT K. Roslin Dayana roslin.moncy@gmail.com Department of Computer Science and Engineering, R.M.D. Engineering College, R.S.M. Nagar, Kavaraipettai, Gummidipoondi Taluk, Thiruvallur 601206, TN, India

performing any data operations. The highlights of this paper are as follows:

- Role-based access control is enforced, such that data access permission is granted based on the roles.
- Data encryption is performed by the Data Owner (DO) before outsourcing, such that the decryption is necessary for gaining access to the data.
- Trust value is set for the users and the access grants are modified in line with it.

The remaining contents of this paper are organized in the following model. Section 2 discusses the related literature with respect to access control mechanisms for cloud data access and the proposed RBAC model with encryption is presented in Section 3. Section 4 ascertains the performance of the proposed work and the concluding remarks are highlighted in Section 5.

2. Review of literature

The related works concerning access control policies of cloud data are discussed in this section.

Numerous research accomplishments have been made in cloud access control, which basically consists of three different domains. In cloud security, access control is the most fundamental way to have control over the outsourced data. In this day and age of big data, more focus is placed on the safety of the information content as well as its storage [13,14] and the literature provides a wide range of access control models, which are based on task, attributes, usage control (UCON), Bell-LaPadula (BLP) based, and so on.

In [15], RBAC and attribute-based access control (ABAC) are combined. The attributes of ABAC were used in the lower layer to automatically generate RBAC models, while the higher layer of attribute-based access control was made up of RBAC. The authors of the article [16] proposed a novel UCON model as a potential solution to the issue of variable subject attribute in the cloud. Within the framework of an access control system based on UCON, this was carried out.

It is stated in reference [17] that a virtual machine system can be constructed using the BLP paradigm. This technology made it simple to isolate virtual machines and allowed for effective collaboration. Within the framework of BLP-based access control, this action was taken. Second, [18] proposed a framework for user authentication and privacy preservation of data stored in the cloud. Additionally, after the completion of authentication process, ABE encryption storage of data can be carried out. This was done in order to ensure that the authentication process could take place after the ABE encryption storage of data.

Multi-authorization centre access control mechanism is presented in reference [19], as well as a certificate authority (CA) that maintains the unique user and authorization identifiers (UID, AID) for each user. Li et al. [20] suggested a paradigm for multi-tenancy that was based on access control. This model was intended to address the challenges of multi-tenancy and virtualized access control in the cloud. In reference [21], the idea of role-based multi-tenant access control, also abbreviated as RB-MTAC, was dreamed of and designed. Through the utilization of user identity management, this model is able to identify user identification and applicable responsibilities. Additionally, it achieves data and programme isolation through the efficient administration of tenant access rights. The ultimate purpose of this paradigm is to enhance the level of multi-tenant security and privacy that is present in cloud-based systems. In reference [22], the concept of a hypervisor-based multi-tenant access control system known as CloudPolice was presented. CloudPolice took advantage of the hypervisor so that the access control policies for the virtual machines could be dynamically coordinated.

A solution that uses access control that is based on roles and attributes for data exchange across services is provided in [23]. This solution allows for the preservation of users' privacy when sharing data, as well as the identification and prevention of data leakage. These services may include those that are stored in surroundings that are not considered to be trustworthy. The method makes use of Active Bundles (AB), the contents of which contain key-value pairs whose values are stored in encrypted form, metadata, access control policies, and a policy enforcement engine. The values of the key-value pairs are also encrypted. The active bundle technique protects the data from the prying eyes of potentially hostile cloud administrators by ensuring the data's secrecy as well as its integrity. This shields the data from potential threats posed by cloud administrators. Once the data leakage detection system was put into place, it was discovered that it resulted in a performance overhead of between 60% and 8%.

Liu et al. [24] outline a mechanism for controlling data access that is both just and fair in the context of cloud storage. The system performs a fair key reconstruction in order to prevent illegal access to shared data, and none of the users sold their shares with one another. This ensures that the data cannot be accessed by unauthorized parties. The method that has been suggested for concealing the data decryption key that is exchanged entails the development of a substantial number of bogus keys. The investigation of this scheme from a theoretical perspective uncovered the fact that all of the shares are always donated by their respective users, which enables those users to reassemble the fair decryption key each time it is used. The fact that every single one of the shares is always given by the corresponding users was the deciding factor in this case. The performance evaluation also revealed that the computation time and communication costs had lowered, but

the authentication method did not operate very well inside the scheme. This was despite the fact that both of these metrics had been shown to have improved. This was demonstrated by the fact that the authentication process for users required significantly more time.

For application in mobile cloud computing, Li et al. [25] suggested a lightweight data sharing method. LDSS was able to successfully enhance access control tree structure by making use of the CP-ABE method, which was developed with the intention of stimulating the mechanism that is pertinent for mobile cloud environments. Within the context of this particular system, the responsibility for a sizeable portion of the processing is moved away from mobile devices and onto proxy servers located on the internet. When users in mobile cloud settings share data with one another, the overhead on the LDSS implementation on the mobile device side is reduced, which in turn results in a reduction in the amount of work that needs to be done.

A threshold multi-authority CP-ABE access control method called TMACS is presented in [26] for use in public cloud storage. This mechanism is recognized by its acronym, TMACS. This technique makes it possible for multiple authorities to collaborate on the administration of a consistent attribute. A combination of the classic multi-authority scheme and the TMACS scheme is employed. This is done so that the characteristics set can be handled, as well as so that security and system-level robustness can be achieved. In this system, a subset of the entire attribute set is jointly maintained by attributes that come from a variety of various authority sets as well as several authorities that are contained within the same authority set.

The authors of the article [27] construct a hierarchical access control system that provides inheritance of permission in order to reduce the burden and risk that would otherwise be incurred in the event of a single authority. This is done in order to lower the load that would be incurred by the case of a single authority. The problem of ciphertext size being linearly dependent on the number of attributes is addressed by the approach by employing CP-ABE in conjunction with a constant-size ciphertext. In addition, the system maintains a consistent value for the size of the ciphertext as well as the computation required for encryption and decryption. This helps to reduce the additional overhead that is associated with the storage of space, the transmission of data, and the computation.

DaSCE is the name of a proposed data security system that was proposed by Ali et al. [28] for protecting data that is hosted in the cloud. This system provides (a) administration of keys, (b) control over who can access files, and (c) guaranteed deletion of previously stored data. The method makes use of Shamir's threshold concept, which allows for the keys to be managed in an organized fashion. Validity of policies is required in order to ensure that access control is kept to both the data and the key. The availability of associated policies in conjunction with the data that users upload to cloud storage serves as the foundation for assured erasure.

In [29], virtual resource management approaches are presented for a cloud environment. These methodologies involve building a RBAC policy, which lowers the possibility of data being exposed to unauthorized parties. These approaches contribute to maintaining the confidentiality of sensitive information. In multi-tenant data centres, the idea of sensitivity is utilized when discussing the degree to which individual tenants share their data with one another. It is generally accepted that data centres with low levels of information sharing have low levels of sensitivity, whereas data centres with high levels of information sharing are generally accepted to have high levels of sensitivity.

Xu et al. [30] came up with a plan for dynamic user groups and on-demand services that included a fine-grained access control method as well as a data-sharing protocol. The operation of this system is accomplished by (1) denying and enforcing access regulations based on the data attributes; (2) allowing the key generation centre to update user credentials; and (3) allowing untrusted CSPs to conduct computation activities without requiring any delegation key.

The method that is proposed in [31] for the goal of providing a time and attribute factors combined access control on time-sensitive data for public cloud storage (TAFC) is known as Embedding Timed-Release Encryption (TRE) into Ciphertext-Policy Attribute-based Encryption (CP-ABE). The owners of the data have the ability, through the use of this scheme, to flexibly release access rights to a variety of users at a variety of times in accordance with a well-defined access policy over the attributes and release time. The owners of the data have the option of encrypting their information using this approach as well.

Motivated by the existing solutions, this paper presents a trust-based encrypted RBAC system for secure cloud data storage, which is explained in the forthcoming section.

3. Proposed trust-based cryptographic RBAC system for cloud data storage

In a cloud data storage system, data owners can set access policies, and cloud providers must follow them. Before uploading data to the cloud, data owners can encrypt it so that only authorized users can access it. Cryptographic systems implement access controls on outsourced data. These outsourced data privacy systems use cryptography and access control. Considering this point, this work employs trust measure to determine the dignity of the user with a specific role and grants permission accordingly. This section intends to explain the different entities present in the system and trust degree computation with respect to different roles.

Table 1. Annotations and symbols.

Abbreviation/ symbol	Meaning
SA	System administrator
DO	Data owners
R	Role
RBAC	Role-based access control
AES	Advanced encryption standard
U_{AP}	Access policy violation by user
U_{IA}	Illegitimate activity by user
$AH(R)$	Access history
H_i^R	Historical record of transaction of DO
$Tran_s$	Transactions with positive feedback
$T_\delta(R)$	Individual trust degree
(TV_k, R)	Collection of all trust vectors in $AH(R)$ with respect to role R
W_o	Weight (positive integer)

The overall annotations of the utilized symbols and abbreviations are shown in Table 1.

3.1. Components of the proposed system

The proposed trust-based RBAC system on encrypted data involves four major entities such as System Administrator (SA), users, Data Owners (DO) and roles, which are discussed as follows:

- SA: The RBAC system relies on the administrator to act as the system's certificate authority. The administrator is responsible for producing the system parameters and distributing all of the required credentials. In addition to this, the administrator is responsible for managing the system's role-based hierarchical structure. They are kept on the cloud and are made accessible to the general public.
- Users: Users are the individuals or organizations that are interested in obtaining specific data from the cloud. When a user wants to access data that has been stored in the cloud, a request has to be sent to the cloud, and then, after receiving a response from the cloud, the user can decrypt the data.
- DO: The parties who are in possession of the data and who wish to store it in an encrypted form in the cloud for other users to access are known as DOs. Within the context of role-based policies, DOs determine who is permitted to view the data. They are the parties that are responsible for managing the relationship between the roles and permissions in the RBAC paradigm. A DO may be a user within the organization or an external party who wishes to communicate data to users within the organization. Both scenarios are possible. In this design, a DO is considered to be a component that is logically distinct from a user, despite the fact that a user can function in the role of a DO and vice versa.
- Roles: Users and DOs are connected to one another by roles, which are abstract entities. Each position possesses its unique set of role parameters that, when combined, establish the user membership for that role. These role parameters are saved in the cloud, and in order to update the user membership of a role, a role needs to make the appropriate changes to these role parameters in the cloud.

Hence, when a DO wants to outsource its data, the data has to be encrypted by the previous phase of work based on keccak and Advanced Encryption Standard (AES) algorithm [32]. The encrypted data is stored in the cloud and the DO decides the access pattern of the data concerning the roles. The SA maintains the role structure and takes care of the access model of the outsourced data then. The user can access the data based on his/her access level of data. When the user is granted with access permission, the encrypted data alone can be accessed, after which decryption is done by the user. The trust degree of the user is computed by considering the attitude of the user.

This work considers two cases of user misconduct. In the first case, the user tries to break the access policy and proceeds against the privilege (U_{AP}). In the second case, the user involve in illegitimate activities such as data leakage (U_{IA}). Both these cases are considered and get reflected in the trust degree. The trust degrees are maintained by the SA and the construction of trust vector is as follows:

$$TV = (Tran_s, U_{AP} + U_{IA}) \tag{1}$$

The user activity monitoring agent tracks the behaviour of the user and the computed trust degrees are stored in a local database. The trust degrees of users are accessible to DOs. The access history of the users with respect to roles is denoted by

$$AH(R) = \{H_1^R, H_2^R, \ldots, H_n^R\} \tag{2}$$

$$H_i^R = \langle ID_i, tv_i, R\rangle \tag{3}$$

$$tv_i, R = (Tran_s, U_{AP}, U_{IA}) \tag{4}$$

Here the trust vector H_i^R indicates the historical record of transaction of DO with identifier ID_i with role R. $Tran_s$ indicates the transactions with positive feedback, U_{AP} and U_{IA} represent transactions with access violation and illegitimate access leading to negative feedbacks.

For instance, when a DO under role "R" is assigned with a resource, then the user activity monitoring agent increments the value of '$Tran_s$' by 1. However, when the DO involves in U_{AP} or U_{IA}, then the value is decremented by 1. Considering the misuse, the U_{AP} or U_{IA} is incremented by 1.

In order to compute the trust degree of a role R, the historical records are obtained and the individual trust degree is computed by:

$$T_\delta(R) = (TV_k, R) \tag{5}$$

$$(TV_k, R) = TV_{k,R} + W_o \sum_{i=1}^{n} tv_i, R \qquad (6)$$

In the above equations, TV_k, R is a collection of all trust vectors in $AH(R)$ with respect to role R. The weight W_o is a positive integer, which indicates the user's data access record and its associated trust value.

A local database is used in the trust models, and within it, all of the interaction histories and trust records that are associated with roles and users are kept. The SA uses the records of all of these interaction histories and trust records to determine the trust value of roles and users. These records are kept in the local database, which is utilized to keep track of the records. Any entity that is located outside of the trust management system will be unable to access the local database when it is needed.

A User activity monitoring agent gathers feedbacks for roles from their respective owners in order to maintain the reliability of the information contained within the feedbacks on roles. It is the responsibility of the User activity monitoring agent to verify the legitimacy of an owner before they are allowed to upload feedback. The local database gets all of the feedbacks that are valid, while any feedbacks that aren't valid will be discarded. The User activity monitoring agent compiles information regarding the data that is assigned to roles. When DO encrypt data that is assigned to roles, they are obligated to notify the User activity monitoring agent. The number of resources that have been allotted to the roles will be updated in the local database by the agent.

In addition, the User activity monitoring agent pays attention to feedback in two ways. The first comes from the roles that have the ability to detect data leakage, and the second comes from the user activity monitoring agent, which reports the access histories of users to the data that is stored in the cloud. This agent assesses whether a user is implicated in the leakage of data, and if the user has viewed the leaked data, the user trust records will be updated in the local database. The overall flow of the proposed approach is presented as follows:

(1) User memberships and role-related settings are forwarded to the cloud.
(2) The DO encrypt and upload the data to the cloud server.
(3) When user needs data access, the request is forwarded to User activity monitoring agent.
(4) The User activity monitoring agent forwards the request along with user and resource identifiers to the Cloud Server (CS).
(5) When the user wants to modify the data, a request is sent to User activity monitoring agent and the DO is notified of the same along with the trust degree of the user.
(6) On DO's approval, the user can modify and upload the data. On completion of the process, the agent is notified.
(7) When data leakage is detected by DO, then the User activity monitoring agent is notified and the local database is updated with respect to resource and user identifiers.
(8) The trust record is updated and the users who have accessed that particular resource are notified.
(9) In case of misconduct, the SA revokes the membership of the user.

Table 2. Illegitimate user detection rate analysis with trust degree utilization.

Performance measures/methods	Without trust	With trust
Accuracy (%)	93.2	**98.8**
Precision (%)	90.3	**96.4**
Recall (%)	86.3	**93.7**
F-measure (%)	88.25	**95.03**
Time consumption (s)	9.8	**4.2**

The achieved values of the proposed work are highlighted in bold.

Hence, the step-wise explanation of the proposed work is given and the performance of the work is evaluated in the following section.

4. Results and discussion

The task is emulated using the Java platform on a computer with an Intel i7 processor running at 1.80GHz and 16GB of random access memory (RAM). The simulation is run on ten separate cloud servers, and the data are dispersed to each of them. This work is now processing data totalling 500MB in size. The effectiveness of this job is assessed based on its illegitimate user detection, memory consumption, storage utilization, and the amount of time required for data storage and retrieval.

Illegitimate user detection is the main theme of this work, such that the privilege is revoked and Table 2 shows the accuracy of detection. Memory use is another crucial condition that must be met by any method. In order for the effectiveness of the suggested algorithm to be asserted, the amount of memory that is used should ideally be kept to a minimum.

The usage of storage comes into play here since this work employs User activity monitoring agent for computing the trust degree of the user and managing it. Therefore, the amount of storage space utilized in relation to the CS is measured. In addition to this, it is essential to determine how much time is required to both store and retrieve the data from the CS.

From Figure 1, it is evident that the proposed work detects the illegitimate users better by employing trust degree. Here, two cases of user misconduct is considered, which are access policy violation and data leakage. The proposed work effectively detects the illegitimate users and revises their access policies, which in turn

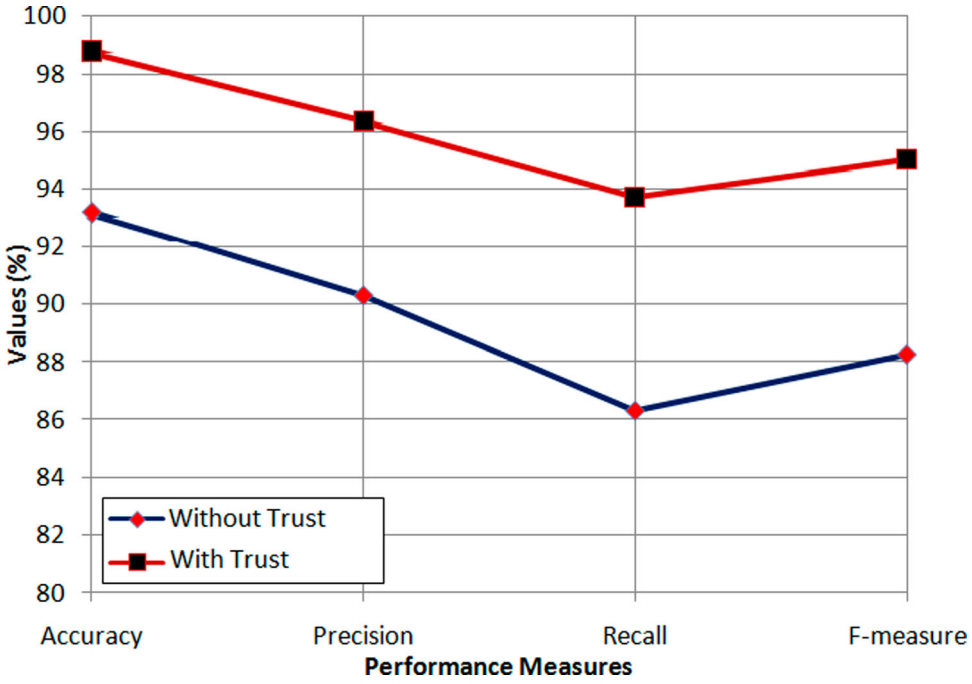

Figure 1. Illegitimate user detection rate analysis.

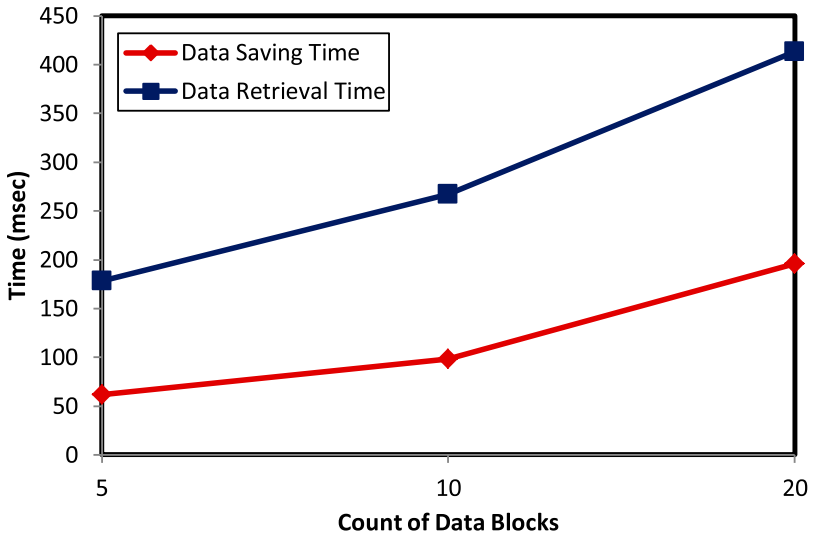

Figure 2. Data storage and retrieval time.

Table 3. Memory consumption analysis (%).

Data (MB)/techniques	50	100	150	200
Without trust	9	11	14	18
With trust	16	20	24	27

preserves the data integrity. The memory consumption analysis is shown in Table 3.

The memory consumption of the proposed work is slightly greater and it grows with data. The maintenance of historical records of data access in local database and trust-related information, which is quintessential for illegitimate user detection, increases the memory consumption. On the other hand, when the work does not check for any such criteria, then the memory consumption is minimal, as shown in Table 3. The data storage and retrieval time is shown in Figure 2.

Calculations have been done to determine how long it takes to save and retrieve all 500 MB of data, and the findings have been reported. At first, the full 500 MB is split up into five 100 MB chunks, ten 50 MB chunks, and twenty 25 MB chunks. The findings of the experiment indicate that the amount of time spent saving data is significantly less than the amount of time spent retrieving data. Since the amount of time required to retrieve the data is evaluated based on how long it takes to retrieve all of the data, this indicates that the amount of time required is greater. In addition to this, the sequence needs to be preserved while the data is being retrieved.

On the other hand, the retrieval process is carried out in a streak whenever just one particular data block at a time is accessed. The amount of time necessary to store data and retrieve it grows proportionally with the number of data blocks. The amount of

Table 4. Comparison with existing works w.r.t access control.

Techniques/performance measures	Accuracy (%)	Precision (%)	Recall (%)	*F*-measure (%)
Attribute-based [27]	92.8	89.4	84.3	86.77
DaSCE [28]	94.6	90.3	86.4	88.3
Time and attribute [31]	97.6	93.2	90.3	91.72
Proposed trust based RBAC	**98.8**	**96.4**	**93.7**	**95.03**

labour associated with it likewise increases proportionally with the number of data blocks that are being processed. Having additional data blocks does, however, provide an increased level of safety, despite the increased computing complexity this entails. Table 4 shows the access control ability of the proposed work in contrast to the existing works. The inclusion of the trust concept performs better, when compared to other works, which improves the overall performance of the proposed work.

5. Conclusions

This article presents a trust-based cryptographic RBAC system for cloud data storage. The entire work is segregated into two phases, where the first phase focuses to encrypt the data to be outsourced and the second phase is meant for providing access to it. This work allows data access by imposing a major entity called User activity monitoring agent, which intends to compute the trust degree of the user and maintain them in local database. Data access decision to a requested user is made by considering the decision of the agent. In this work, two kinds of misconduct affect the trust degree of the user and they are access policy violation and data leakage. The illegitimate users are detected by this approach and the access grant is revoked by the system. The performance of the work is compared with the existing works and the proposed work performs better. In future, dynamic operations on cloud data are to be elaborated.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

[1] Mell P, Grance T. The NIST definition of cloud computing [technical report special publication]. Gaithersburg, MD, USA: National Institute of Standards and Technology; 2011. p. 800–145.
[2] Liu F, Tong J, Mao J, et al. NIST cloud computing reference architecture. NIST Spec Publ. 2011;500(211):1–28.
[3] Wu J, Dong M, Ota K, et al. FCSS: fog-computing-based content-aware filtering for security services in information-centric social networks. IEEE Trans Emerg Topics Comput. 2019;7(4):553–564. doi:10.1109/TETC.2017.2747158
[4] Lin X, Li J, Wu J, et al. Making knowledge tradable in edge-AI enabled IoT: a consortium blockchain-based efficient and incentive approach. IEEE Trans Industr Inform. 2019;15(12):6367–6378. doi:10.1109/TII.2019.2917307
[5] Zhang YQ, Wang XF, Liu XF, et al. Survey on cloud computing security. J Softw. 2016;27(6):1328–1348. doi:10.13328/j.cnki.jos.005004
[6] Namasudra S, Roy P. Secure and efficient data access control in cloud computing environment: a survey. Multiagent Grid Syst. 2016;12(2):69–90. doi:10.3233/MGS-160244
[7] He P, Huang R, Chen N, et al. Research progress on side-channel attacks in cloud environment. Appl Res Comput. 2018;35(4):969–973.
[8] Liang W, Yang Y, Yang C, et al. PDPChain: a consortium blockchain-based privacy protection scheme for personal data. IEEE Trans Reliab. 2022;72:586–598. doi:10.1109/TR.2022.3190932
[9] Gupta I, Saxena D, Singh AK, et al. Secom: an outsourced cloud-based secure communication model for advanced privacy preserving data computing and protection. IEEE Syst J. 2023: 1–12. doi:10.1109/JSYST.2023.3272611
[10] Singh AK, Saxena D. A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment. J Appl Secur Res. 2022;17(3):385–412. doi:10.1080/19361610.2020.1870404
[11] Gupta R, Gupta I, Saxena D, et al. A differential approach and deep neural network based data privacy-preserving model in cloud environment. J Ambient Intell Humaniz Comput. 2023;14(5):4659–4674. doi:10.1007/s12652-022-04367-x
[12] Saxena D, Gupta I, Gupta R, et al. An AI-driven VM threat prediction model for multi-risks analysis-based cloud cybersecurity. IEEE Trans Syst Man Cybernet Syst. 2023: 1–13. doi:10.1109/TSMC.2023.3288081
[13] Yu K, Eum S, Kurita T, et al. Information-centric networking: research and standardization status. IEEE Access. 2019;7:126164–126176. doi:10.1109/ACCESS.2019.2938586
[14] Qi X, Su Y, Yu K, et al. Design and performance evaluation of content-oriented communication system for IoT network: a case study of named node networking for real-time video streaming system. IEEE Access. 2019;7:88138–88149. doi:10.1109/ACCESS.2019.2925885
[15] Huang J, Nicol DM, Bobba R, et al. A framework integrating attribute-based policies into role-based access control. In: Proceedings of the 17th ACM Symposium on Access Control Models and Technologies (SACMAT). New York, NY: ACM; 2012. p. 187–196.
[16] Tavizi T, Shajari M, Dodangeh P. A usage control based architecture for cloud environments. In: Proceedings of the 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum. 2012. p. 1534–1539. doi:10.1109/IPDPSW.2012.193
[17] Lin G, He S, Huang H, et al. Access control security model based on behavior in cloud computing environment. Acta Autom Sin. 2012;33(3):59–66.

[18] Ruj S, Stojmenovic M, Nayak A. Privacy preserving access control with authentication for securing data in clouds. In: Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing (CCGRID). 2012. p. 556–563. doi:10.1109/CCGrid.2012.92

[19] Yang K, Jia X. Attributed-based access control for multi-authority systems in cloud storage. In: Proceedings of the 2012 IEEE 32nd International Conference on Distributed Computing Systems. 2012. p. 536–545. doi:10.1109/ICDCS.2012.42

[20] Li X-Y, Shi Y, Guo Y, et al. Multi-tenancy based access control in cloud. In: Proceedings of the International Conference on Computational Intelligence and Software Engineering. 2010. p. 1–4.

[21] Yang S-J, Lai P-C, Lin J. Design role-based multi-tenancy access control scheme for cloud services. In: Proceedings of the International Symposium on Biometrics and Security Technologies. 2013. p. 273–279.

[22] Popa L, Yu M, Ko SY, et al. CloudPolice: taking access control out of the network. In: Proceedings of the 9th ACM SIGCOMM Workshop Hot Topics Networks (HotNets). New York, NY: ACM; 2010. p. 1–6.

[23] Ulybyshev D, Bhargava B, Oqab-Alsalem A. Secure data exchange and data leakage detection in an untrusted cloud. In: Applications of Computing and Communication Technologies. Singapore: Springer; 2018. p. 99–113.

[24] Liu H, Li X, Xu M, et al. A fair data access control towards rational users in cloud storage. Inf Sci. 2017;418–419:258–271. doi:10.1016/j.ins.2017.07.023

[25] Li R, Shen C, He H, et al. A lightweight secure data sharing scheme for mobile cloud computing. IEEE Trans Cloud Comput. 2018;6(2):344–357. doi:10.1109/TCC.2017.2649685

[26] Li W, Xue K, Xue Y, et al. TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage. IEEE Trans Parallel Distrib Syst. 2016;27(5):1484–1496. doi:10.1109/TPDS.2015.2448095

[27] Teng W, Yang G, Xiang Y, et al. Attribute-based access control with constant-size ciphertext in cloud computing. IEEE Trans Cloud Comput. 2017;5(4):617–627. doi:10.1109/TCC.2015.2440247

[28] Ali M, Malik SUR, Khan SU. DaSCE: data security for cloud environment with semi-trusted third party. IEEE Trans Cloud Comput. 2017;5(4):642–655. doi:10.1109/TCC.2015.2446458

[29] Almutairi A, Sarfraz MI, Ghafoor A. Risk-aware management of virtual resources in access controlled service-oriented cloud datacenters. IEEE Trans Cloud Comput. 2018;6(1):168–181. doi:10.1109/TCC.2015.2453981

[30] Xu S, Yang G, Mu Y, et al. Secure fine-grained access control and data sharing for dynamic groups in the cloud. IEEE Trans Inf Forensics Secur. 2018;13(8):2101–2113. doi:10.1109/TIFS.2018.2810065

[31] Hong J, Xue K, Xue Y, et al. TAFC: time and attribute factors combined access control for time-sensitive data in public cloud. IEEE Trans Serv Comput. 2020;13(1):158–171. doi:10.1109/TSC.2017.2682090

[32] Roslin Dayana K, Shobha Rani P. Secure cloud data storage solution with better data accessibility and time efficiency. Automatika. 2023;64(4):751–758. doi:10.1080/00051144.2023.2213564