Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 13, Issue 1, January 2022: 204-211

Enhancing Role Based Access Control with Privacy in Cloud Computing

K.Mythili[a], S. Rajalakshmi[b]

[a]Assistant Professor, CSA Department, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya, Enathur, Kancheepuram.
[b]Professor, CSE Department, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya, Enathur, Kancheepuram.

Abstract

Cloud Computing provides high performance, accessibility and low cost for data storing and sharing, provides a better consumption of resources. Cloud service providers compromise an abstraction of infinite storage space for clients to mass data. However, security concerns are the main constraints as we now outsource the storage of data possibly sensitive to cloud providers. To preserve data privacy, a mutual approach is to encrypt data files before the clients upload the encrypted data into the cloud. Data confidentiality becomes the main concern in outsourcing client data to cloud storage and it is also essential for an access control mechanism to prevent data mistreatment within the organization. There is no system designed for secure and efficient data sharing especially for dynamic groups in the cloud. Therefore we propose a secure data sharing scheme by using Role based Access Control (RBAC) and Elliptical Curve Cryptography (ECC) for frequently changed groups and anonymous access. RBAC provides flexible controls and database management by having users mapped to roles and roles mapped to privileges on data objects. ECC based encryption scheme incorporates the cryptographic approaches. ECC with RBAC provides anonymous access control, thereby to address the privacy in data as well as the user identity. If the group member is revoked, this system provides automatic generation of new public key of existing group and distributed to the group, which eliminate the need to encrypt the data again with this new key therefore any user in the group can access the data in the cloud, which is not accessible by the revoked users. Thus the proposed method provides privacy and data confidentiality in cloud.

Keywords: Data Privacy, Data Confidentiality, Access control Mechanism

1. Introduction

The first way a system provides security to its resources and data, is by controlling access to the resources and the system itself. However, access control is more than just controlling which users (subjects) can access which computing and network resources. In addition, access control manages users, files and other resources. It controls user's privileges to files or resources (objects). In access control systems various steps like, identification, authentication, authorization and accountability are taken before actually accessing the resources or the object in general. In early stages of computing and information technology, researchers and technologists realized the importance of preventing users from interfering each other on shared systems. Various access control models were developed.

User's identity was the main index to allow users to use the system or its resources. This approach was called Identification Based Access Control (IBAC). However, with the growth of the networks and the number of users, IBAC was found to be weak to defend such a large growth. Advanced concepts in access control were introduced which included owner/ group/ public. IBAC proved to be problematic for distributed systems as well. Managing access to the system and resources became hard and vulnerable to errors. A new method known as Role Based Access Control (RBAC) was introduced. Role based Access Control (RBAC) determines user's access to the system based on the Job role. The role a user is assigned to be basically based on the least privilege concept. The role is defined with the least amount of permissions or functionalities that is necessary for the job to be done. Permissions can be added or deleted if the privileges for a role change.

Elliptic Curve Cryptography (ECC) is a strategy to public-key cryptography established on the algebraic constitution of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (centered on undeniable Galois fields) to provide similar security. Elliptic curves are applicable for key contract, digital signatures, pseudo-random generators and different duties. Elliptic curve cryptography (ECC) is a public key encryption method established on elliptic curve that can be utilized to create rapid, smaller, and more effective cryptographic keys. ECC generates keys by means of the elliptic curve equation instead of the typical approach of new release because the product of very tremendous prime numbers. In accordance to some researchers, ECC can yield a stage of safety with a 164-bit key for the systems which requires 1,024-bit key to achieve. Thus ECC helps to establish similar protection with least power consumption.

2. Existing System

Nowadays, privacy preserving is playing important role in cloud computing where content based privacy is challengeable task in untrusted cloud environment. Based on literature studies, there are some techniques available to content based privacy like DES, AES, ABE, CP-ABE and KP-ABE. However, they are being quite dull to maintain the efficiency of key generation, encryption and decryption process. Current approaches still believe in user identity, mutual privacy and key agreement session wise among Content Owner, Trusted Client, and Cloud Service Provider. Certificate authority based Kerberos Protocol is utilized to apply certificate based authorization. Still, key complexity, malicious attack activity, and data continuity with minimal setup is challenged.

3. Review of Related Works

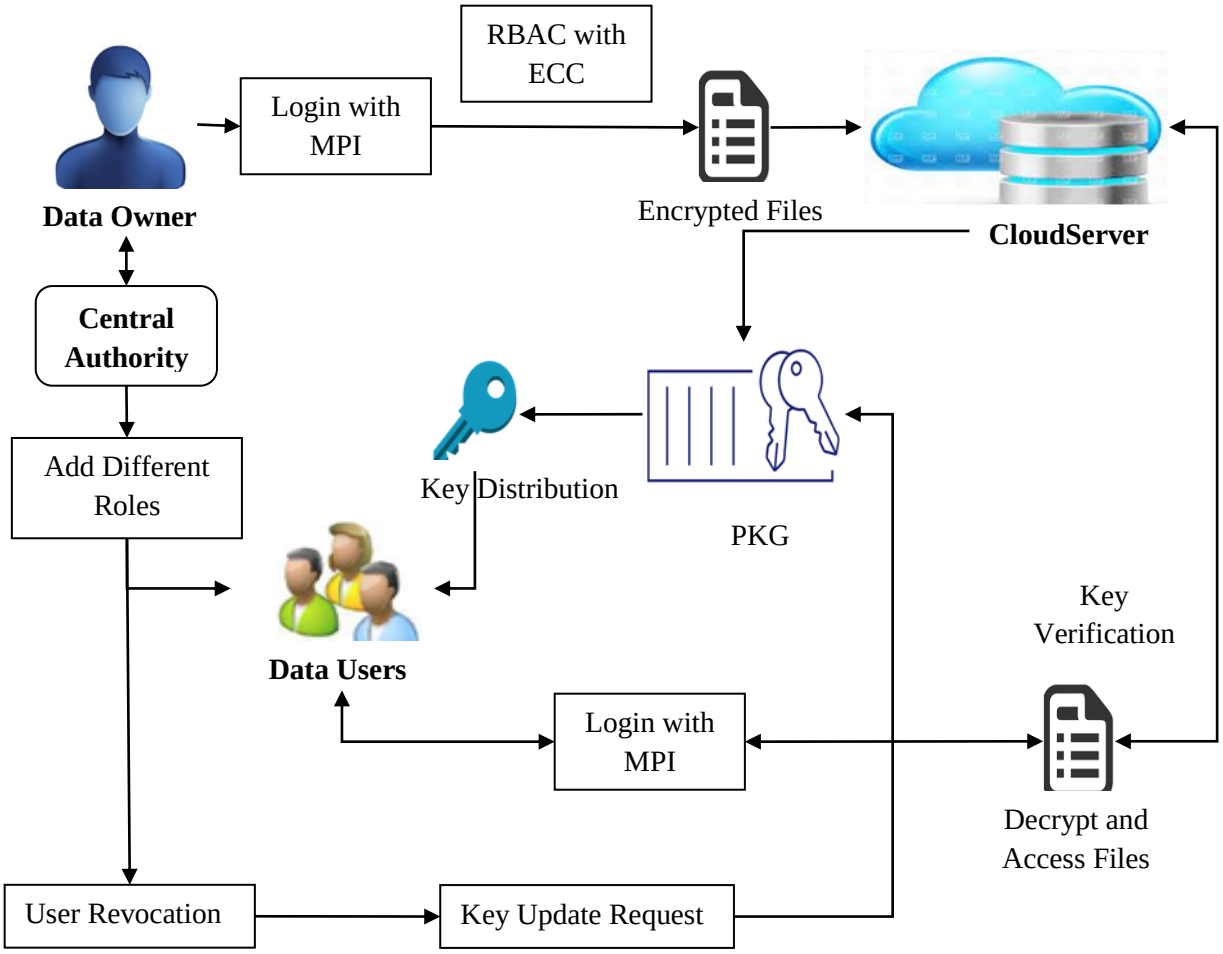
Depavath Harinath (2015) –" Enhancing Data Security Using Elliptic Curve Cryptography in Cloud Computing" proposes a data security model that uses Elliptic curve cryptosystem for digital signature. Digital Signature Scheme and Public Key Cryptography are integrated to enhance the security level of Cloud, aiming to identify the most vulnerable security threats in cloud computing, which will enable both end users and vendors to know about the key security threats and the issues associated with cloud computing[1]. ***Divya Pritam and Madhumita Chatterjee (2016) - "Enforcing Role-Based Access Control for Secure Data Storage in Cloud Using Authentication and Encryption Techniques"*** proposed a novel encryption scheme which incorporates the cryptographic approaches with RBAC and also an anonymous control scheme to address the privacy in data as well as the user identity privacy in current access control schemes. For secure cloud

environment, the following methods were proposed by (author's name) to protect user's privacy and security of data: (1) Two-tier authentication to protect the confidentiality of the Data owner and Data User (2) deploying an admission control policy to provide feedback voting for new Data Owner (3) storing the data after encryption (4) RBAC policy to control the usage of Data Owner's data[2]. ***Anmin Fu, Yuqing Zhang, Huaqun Wang, and Chanying Huang (2017) – "NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users"*** Propose a new privacy-aware public auditing mechanism for shared cloud data by constructing a homomorphic verifiable group signature. It requires at least t group managers to recover a trace key cooperatively, which eliminates the abuse of single authority power. Group users can trace the data changes through the designed binary tree and recover the latest correct data block when the current data block is damaged[3]. ***Jiang, Tao, Xiaofeng Chen, and Jianfeng Ma (2015) - "Public integrity auditing for shared dynamic cloud data with group user revocation."*** proposed scheme is designed to solve the security and efficiency problems of public data integrity auditing with multi-user modification, where the data has to be encrypted among a dynamic group and any group user can conduct secure and verifiable data update when necessary. Thus the building blocks are secure, which include the vector commitment, group signature, and asymmetric group key agreement scheme[4]. ***Jianghong Wei, Wenfen Liu, and Xuexian Hu(2016) - "Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage"*** proposed to build a secure and cost-effective multiauthority attribute-based access control scheme for data sharing in cloud storage systems, It is a multiauthority CP-ABE scheme supporting scalable user revocation and public cipher text update[5]. ***Lan Zhou, Vijay Varadharajan, and Michael Hitchens(2013) - Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage"*** proposed a role-based encryption (RBE) scheme that integrates the cryptographic techniques with RBAC. it allows RBAC policies to be enforced for the encrypted data stored in public clouds. This system captures practical access policies based on roles in a flexible manner and provides secure data storage in the cloud enforcing these access policies [6]. ***Shilpi Harnal, R.K. Chauhan(2019) - "Efficient and Flexible Role-Based Access Control (EF-RBAC) Mechanism for Cloud"*** proposed an Efficient and Flexible Role-Based Access Control (EF-RBAC) mechanism for the cloud computing environment to achieve confidentiality and security. RBAC limits the accesses for resources within an organization to authorized users only and also guarantees that a user can solely access specific information they are authorized for the organization policy [7]. ***Rubina Ghazal, Ahmad Kamran Malik, Nauman Qadeer, Basit Raza, Ahmad Raza Shahid and Hani Alquhayz(2020) "Intelligent Role-based Access Control Model and Framework Using Semantic Business Roles in Multi-domain Environments"*** proposed novel access control framework that uses semantic business roles and intelligent agents through implementation of our Intelligent RBAC (I-RBAC) model. It encompasses occupational entitlements as roles for multiple domains. This method combines the core I-RBAC ontology using real-world semantic business roles and intelligent agent technologies for achieving required level of access control in highly dynamic multi-domain environment [8].

4. Proposed Architecture

The figure1 shows the architecture of proposed secure cloud storage system, a hybrid cloud comprising private cloud which is used to store sensitive role hierarchy and public cloud stores the encrypted data and public parameters associated with the Role Based Access Control with encryption

system. This framework combines the RBAC and ECC to provide the users who wish to access the encrypted data and the data owners who wish to encrypt their data only can interact with the cloud. The role hierarchy and role mappings related to the organization are maintained in the private cloud which is only accessible to the administrator and who manages the user membership relations. Here secured user revocation process and key updates after revocation are implemented. Therefore, when a user is removed from existing group, group key gets updated and distributed to all users present in current data access pattern.



Thus the proposed work is an integrated one which combines RBAC for authorized accessing of resources and Public Key Encryption Mechanism (ECC based) which provides confidentiality in accessing the resource. Therefore, it decreases the risk of security breaches and data leakage. Also there is provision to prevent the revoked users that he can no longer decrypt those previously accessible data and subsequently encrypted data.

5. Procedural Steps of the Proposed Scheme

5.1 Cloud Framework Construction

It is a hybrid cloud architecture comprising a private cloud which is used to store sensitive role hierarchy. There are three Entities in an RBAC model. First, Data Owner (DO) who intend to share and store their information or resources in the cloud; second, users who need to access the owners'

shared resources; and third, Admin who grants the access levels to registered cloud users to share the resources.

5.2 MPI Verification

MPI defines as the message passing interface that used to exchanging messages to multiple systems in a parallel processing. Here a new approach is proposed to access cloud using login credential and MPI based secret key for secure access of cloud storage. PKG is responsible for generating secret key and use MPI for distribution of secret keys to the user. The secret key sharing based on MPI is the concept of dynamic authentication and verification module in cloud security system.

To protect a secret share and a partial public parameter from modification, we introduce a short signature scheme called. A signature σ is an element of G. The base group G and the generator g are system parameters. We make a little modification in order to use it in our proposed scheme. Let MapToGroup be a hash function h : {0, 1} $*$ → G1. The short signature scheme comprises of three algorithms, key generation, signing and verification, which work as follows:

Key Generation:

Pick random $\delta \xrightarrow{R} Z_p$, and compute V ← δQ.

The public key is $V \in E(F_q{}^{\alpha})$.

The secret key is δ.

Signing:

Given a secret key $\delta \epsilon Z_p$, and a message $M \in \{0,1\}^*$, do:

1) Compute R ← MapToGroup $(M) \in G_1$.

2) Let σ ← δR $\in E(F_q)$.

3) Output the x-coordinate of σ as the signature x on M. Then, x $\in F_q$.

Verification:

Given a public key V $\in G_2$, a message $M \in \{0,1\}^*$, and a signature x $\in F_q$, do:

1) Find a y $\in F_q$ such that σ = (x, y) is a point of order p in E(F_q). If no such y exists, output invalid and stop.

2) Compute R ← MapToGroup $(M) \in G_1$.

3) Test if either e(σ, Q) = e(R, V) or $e(\sigma, Q)^{-1}$ = e (R, V).

If so, output valid; Otherwise, output invalid.

5.3 Data Upload and Encryption

Data Owner(DO) is a cloud client who registers with the CSP (Cloud Service Provider). DO anonymously get authenticated to cloud. DO upload his file in encrypted form to the cloud. The DO has the privilege to Set/Deny access his file to the data users.

5.4 Data User with access policies

The system needs of a given workforce are analyzed with users, grouped into roles based on common job responsibilities and system access needs. Access is then assigned to each person based strictly on their role assignment. Here the Data User (DU) is provided with Role-based Access Control (RBAC) policy. The Data User who wants to download a file, makes request to the Data Owner. Then the data owner has his own privilege to permit/deny his file access. If he decides that particular user to access his file then the secret key with time stamp is distributed to his registered mail through MPI. Thus the data leakage is prevented by the way of allowing data users to access the file only with the key for decryption and limited number of attempts within the given duration for downloading. The central authority has privilege to revoke user. If the user is revoked then no more file can be accessed from cloud. PKG generates new group key and shared with the Data Owner and Cloud Users through the MPI Scheme of key distribution.

6. PERFORMANCE MEASURE:

Table.1. Encryption time and Decryption time are considered as the parameter that is used to estimate the speed of proposed system while working with the cloud users. Here the system performs encryption and decryption. The time estimation is compared with CP-ABE approach and proposed algorithm and the proposed algorithm gives better performance as shown in the table1.

Algorithms	**Time taken for Encryption and Decryption**
ABE	30.5 ms
ECC	2.57 ms

Since the elliptic curve cryptography is efficient and more suitable for lightweight devices as compared with bilinear pairing-based cryptosystem, it reduces the time taken for Encryption and Decryption by providing the advantages of less power consumption with the minimum key size by comparing with other cryptosystems.

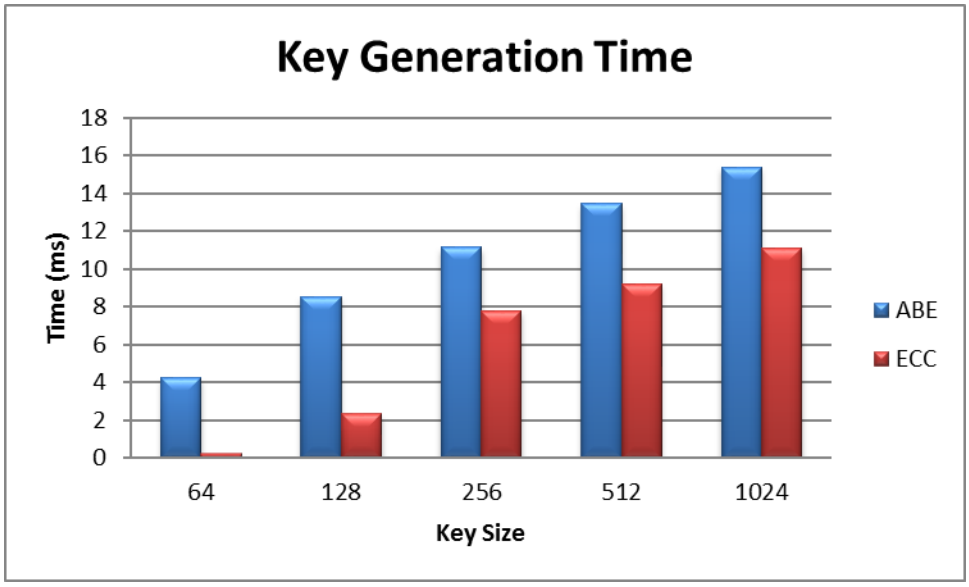
Table.2. Table2 shows the comparison of the proposed model with the ABAC using various parameter such as public key, private key, revocation and key updation.

Access Model	**Access Policy**	**Public Key**	**Private Key**	**Revocation**	**Key Updation**
RBAC	Role Hierarchy	Role Hierarchy and system parameters	Constant Size, specified by role	Dynamic User Revocation	Dynamic key update and sharing
ABAC	Set of Attributes	Set of Attributes and system parameters	Variable size, specified by attribute	None	None

Table.3. Table3 shows the performance comparison with different key sizes and their generation time for the ABE and ECC.

Key-Size(bit)	64	128	256	512	1024
ABE	4.22	8.53	11.13	13.45	15.4
ECC	0.23	2.34	7.8	9.2	11.12

Figure.1. Figure1 shows the performance comparison with different key sizes and their generation time for the ABE and ECC.



7. Conclusion

In this paper, we have proposed a cloud-based storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the CSP, but also updating and scaling this data on the remote servers. There is a need for preventing data breaches from cloud server, thus the proposed scheme enables the authorized users to ensure that they are receiving the secured outsourced data from the cloud with Owner's permission with various checksum of access control based on role and the user also authenticated with the help of MPI to download the document with secret key, time stamp and frequency of secret key. The revoked user is also restricted to download the document from the cloud by updating the key with current existing users. Thus the proposed work provides the safe mode for outsourcing the owner's data in public archives in dynamic cloud environment.

References

[1] Depavath Harinath. (2016) "Enhancing Data Security Using Elliptic Curve Cryptography in Cloud Computing", International Journal of Science and Research, Vol 5, pp 2319-7064.

[2] Pritam, Divya, and Madhumita Chatterjee. (2016) "Enforcing Role-Based Access Control for Secure Data Storage in Cloud Using Authentication and Encryption Techniques." Journal of Network Communications and Emerging Technologies, Vol 6, pp 82-87

[3] Fu, Anmin, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang. (2017) "NPP: a new privacy-aware public auditing scheme for cloud data sharing with group users“, IEEE Transactions on Big Data, pp 1-10.

[4] Jiang, Tao, Xiaofeng Chen, and Jianfeng Ma. (2015) "Public integrity auditing for shared dynamic cloud data with group user revocation“, IEEE Transactions on Computers, Vol 65, pp 2363-2373.

[5] Jianghong Wei, Wenfen Liu, and Xuexian Hu(2016) “Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage”, IEEE Systems , Vol 12, pp 1731-1742.

[6] Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. (2013) "Achieving secure role-based access control on encrypted data in cloud storage“, IEEE transactions on information forensics and security, Vol 8, pp 1947-1960.

[7] Shilpi Harnal, R.K. Chauhan(2019) “Efficient and Flexible Role-Based Access Control Mechanism for Cloud”, EAI Endorsed Transactions on Scalable Information Systems, Vol 7, pp 1-10.

[8] Rubina Ghazal, Ahmad Kamran Malik, Nauman Qadeer, Basit Raza, Ahmad Raza Shahid and Hani Alquhayz (2020) “Intelligent Role-based Access Control Model and Framework Using Semantic Business Roles in Multi-domain Environments”, IEEE Access, Vol 8, pp 12253 - 12267.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in INFOCOM’10, 2010, pp. 534–542.

[10] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang,“Enabling security in cloud storage SLAs with cloudproof,” in Proceedings of the 2011 USENIX conference, 2011.

[11] J. Feng, Y. Chen, W.-S. Ku, and P. Liu, “Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms,” in Proceedings of the 2010 39th International Conference on Parallel Processing, 2010, pp. 251–258.

[12] J. Feng, Y. Chen, and D. H. Summerville, “A fair multi-party non-repudiation scheme for storage clouds,” in 2011 International Conference on Collaboration Technologies and Systems, 2011, pp. 457–465.