ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 2, pp: (148-153), Month: April - June 2019, Available at: www.researchpublish.com

Efficient Approach for Access Control on Public Cloud Storage

[1]S.P. Marke, [2]Y.M. Kurwade, [3]Vilas M. Thakare

[1]S.P. Marke is a student of SGBAU; (e-mail: shrutimarke04@gmail.com).

[2]Y.M. Kurwade is with SGBAU, Amravati, Maharashtra (e-mail: yogeshwarkurwade@gmail.com).

[3]Vilas M. Thakare is with SGBAU, Amravati, Maharashtra (e-mail: vilthakare@yahoo.co.in).

***Abstract*: Cloud computing has become an preferred platform for sharing data among the users all around the world. It's increasing use has brought into concern the security issues. The data being shared is in encrypted form which handles the privacy issue but the data encrypted is more difficult to access by the users. So to solve the issue of privacy as well as access control there should be a more strong scheme which helps the users to securely send their data. In this paper, we have reviewed five different schemes which are : Privacy Preserving Data Processing with Flexible Access Control, RAAC: (Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage), Decentralized Runtime Monitoring for Access Control Systems in Cloud Federations, Privacy preserving Access Control Protocol in Cloud Federations, Fine Grained Access Control Scheme Based on Cloud Storage. These schemes discussed here address the access control in cloud storage but they still have some limitations which need to be handled effectively.**

***Keywords:* Cloud computing, cloud storage, access control, security, privacy, data sharing, encryption, decryption.**

1. INTRODUCTION

The day by day increasing use of the Cloud platform has made it possible to share a large amount of data among the worldwide users. But the security and privacy issues need to be handled. Different methods have been used to overcome the security issues. The sharing of data amongst the users brings the concern of access control so as to decide that which users should be granted the access and which not. There should be methodology for this issue.

There are five different schemes discussed in this paper which are: Privacy Preserving Data Processing with Flexible Access Control, RAAC: (Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage), Decentralized Runtime Monitoring for Access Control Systems in Cloud Federations, Privacy preserving Access Control Protocol in Cloud Federations, Fine Grained Access Control Scheme Based on Cloud Storage.

These several schemes are being used to provide the required Security and access control facilities to the users.

But these schemes have some drawbacks in them, so to overcome the limitations a new improved method "Efficient and Improved Scheme for Access Control and Secure Data Sharing in Public Cloud" is given. This methodology helps to share data in the public cloud securely along with access control rights defined to each user.

2. BACKGROUND

Many studies have been done on the schemes available and their results have been analysed. These schemes ahre given by different authors. The various schemes discussed over here are: Privacy Preserving Data Processing with Flexible Access Control scheme is proposed to enable various computations on the encrypted data in an efficient way and also it able to realize flexible access control. A data service provider is used in this method which helps to realize seven basic operations on the data. It achieves access control without the need of trusted cloud servers [1]. RAAC- Robust and Auditable Access Control with Multiple Authorities for Public Cloud Storage is designed to remove the single—point bottleneck issue and provides fine grained access control to the users in the cloud. A central authority is used to generate secure keys for the user thus enhancing the performance of key generation. Also multiple attribute authorities are there to share the load of user legitimacy verification [2]. Decentralized Runtime Monitoring for Access Control Systems in Cloud Federations scheme is given to implement distributed access control systems. In this it is possible to detect the attacks to the components involved in the system. Also, it is able to find the attacks targeting the integrity of the logs of the monitoring components. [3]. Privacy Preserving Access Control Protocol in Cloud Federations allows the federated organizations to enforce security policies on their data. The users can access these data when their identity attributes matches to the policies but the attributes will not be clear to the organizations. It relies on two novel technologies of blockchain and Intel SGX hardware platform [4]. Fine Grained Access Control scheme based on cloud storage helps to realize safe data sharing of sensitive data in public cloud. It enables the data owner to manage the data effectively and optimizes user revocation. It also helps to reduce the workload and storage space overhead in the cloud environment [5].

This paper introduces five different methods for the secure data sharing and access control facilities for the user. These are: Privacy Preserving Data Processing with Flexible Access Control, Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage(RAAC), Decentralized Runtime Monitoring for Access Control Systems in Cloud Federations, Privacy Preserving Access Control Protocol in Cloud Federations, Fine Grained Access Control scheme.

3. PREVIOUS WORK DONE

In the previous research papers discussed here, various schemes have been discussed for the secure sharing of sensitive data in the cloud environment along with the required access control policies..

Wenxiu Ding et al. (2017) [1] proposed the Privacy Preserving Data Processing with Flexible Access Control for the flexible access control of the encrypted data shared over the cloud. It realizes seven basic operations on the encrypted data which are addition, subtraction, multiplication sign acquisition, absolute, comparison and equality test. It achieves fine grained access control without the need of fully trusted servers. Kaiping Xue et al. (2017) [2] presented the RAAC scheme- Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage which overcomes the single-point performance bottleneck and enables efficient access control scheme with auditing mechanism. In this scheme, a novel heterogeneous framework is given which employs multiple attribute authorities to share the load of user verification. Md Sadek Ferdous et al. (2017) [3] proposed the Decentralized Runtime Monitoring for Access Control Systems in Cloud Federations which is mostly used in cloud federations where different organizations share their data in the cloud so that other users can access data. It makes it possible to detect attacks to the components involved in the access control mechanism. The blockchain technology is used to store logs and perform monitoring checks and it also provides integrity of data, data distribution and control. Shorouq Alansari et al. (2017) [4] proposed the Privacy Preserving Access Control in Cloud Federations that enables the cloud organizations to enforce attribute based access control policies on the data. The users are granted access to the data when their identity attribute matches the policies without the attributes being clear to the system. The two novel technologies used blockchain and SGX hardware platform guarantees the integrity of the policies evaluation process. Xiaojie Niu (2017) [5] gave the Fine Grained Access Control scheme based on cloud storage according to system characteristics of the data storage in cloud. It helps to store sensitive data safely and reduces the time for the data owner to manage the data along with user revocation optimization.

4. EXISTING METHODOLOGIES

There are various schemes available which are being used for providing while sharing sensitive data on the cloud. Also these methods are being implemented for access control mechanism so that users can securely access the required data. These methods discussed over here are : Privacy Preserving Data Processing with Flexible Access Control, Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage(RAAC), Decentralized Runtime Monitoring for Access control Systems in Cloud Federations, Privacy Preserving Access Control Protocol in Cloud Federations, Fine Grained Access Control Scheme Based on Cloud Storage.

4.1 Privacy Preserving Data Processing with Flexible Access Control :

The data which is shared in cloud environment is in encrypted form to give security against intruders. However this data is not easily accessible by all other users. So to give better security and access control, the privacy preserving data processing scheme achieves enhanced access control functionality. It realizes seven basic operations on the data – addition, subtraction, multiplication, sign acquisition, absolute, comparison and equality test. It is based on the Pallier's partial homomorphic encryption and achieves fine grained access control without the need of fully trusted servers. This scheme is efficient working with large amounts of data [1].

4.2 Robust and Auditable Access Control With Multiple Attribute Authorities for Public Cloud Storage (RAAC):

The RAAC scheme is being implemented for removing the performance of single-point performance bottleneck. It gives efficient access control capability with an auditing mechanism. The multiple authorities are used in this to share the load of user legitimacy verification. This methods implements a novel heterogeneous framework along with a central authority which generates secret keys for the verified users. The auditing and tracing mechanism is used to find the misbehaviour of the attribute authorities. Thus this scheme is effectively applicable to all the honest individuals as well as to other users in the cloud [2].

4.3 Decentralized Runtime Monitoring for Access Control Systems in Cloud Federations :

This decentralized runtime monitoring scheme is used in cloud federations where different organizations share their data and services based on their own cloud platform. Due to the distributed nature of the cloud federations this method achieves great accountability and reliability of the access control system. The key feature of this scheme is that it is not only able to detect attacks to the components in access control decision but also senses the attacks that targets the integrity of the logs of the components. It uses the blockchain technology that achieves data integrity, distribution and access control functionality [3].

4.4 Privacy Preserving Access Control in Cloud Federations :

The Privacy Preserving Access Control protocol is used in cloud federations that enables the users to enforce attribute based access control policies on the data in a privacy preserving fashion. The users are granted access to the data only when their identity attributes matches the access policies and without their attributes being revealed. The novel identity and access management architecture is used here as a part of Federation-as-a-Service (Faas). This architecture reline on two technologies –blockchain and Intel SGX hardware platform. It uses cryptographic protocol that guarantees integrity of the data and access control components for evaluating and enforcing policies. Thus this scheme helps to achieve the required access control so that which users can access which data [4].

4.5 Fine-Grained Access Control Scheme Based on Cloud Storage :

In cloud environment, for data sharing security is major issue which needs to be handled properly. For this the Fine Grained Access Control scheme is applied it on cloud storage system with fine grained access control based on CP-ABE. The scheme discussed here optimizes the user revocation, reduces the time of data owner to manage data and realizes the safe and effective storage of sensitive data on the cloud [5].

5. ANALYSIS AND DISCUSSION

The Privacy Preserving Data Processing scheme with Flexible Access Control is used to realize seven different operations on the encrypted data. It integrates attribute based encryption with homomorphism to achieve flexible access control and better security [1]. The RAAC scheme is being implemented to remove the single point performance bottleneck. The multiple attribute authorities share the load of user verification and also the tracing feature helps to find out the misbehaviour of the authorities [2]. Decentralized Runtime Monitoring achieves access control capability of systems in the cloud federations. It is able to detect the attacks in the access control system and to the integrity of the logs of components [3]. The Privacy Preserving access control protocol is used in the cloud federations to achieve better access control by enforcing attribute based access control policies and users get access only when their identity attributes matches the policies. Thus the data integrity and privacy is achieved [4]. The Fine- Grained access control scheme is implemented to optimize the user revocation and reducing time for data owner to manage data. This realizes safe data sharing and efficient storage of sensitive data in public cloud [5].

TABLE 1: Comparisons between different security schemes

Mobility scheme	**Advantages**	**Disadvantages**
Privacy Preserving Data Processing with Flexible Access Control	This scheme realizes seven operations on the encrypted data and achieves better access control for big data processing operations.	.The implementation is a bit complicated.
Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage(RAAC)	The RAAC scheme provides better performance for access control with an auditing mechanism over the traditional CP-ABE scheme	The efficiency is a little slower.
Decentralized runtime Monitoring for Access Control Systems in Cloud Federations	This scheme promotes the better accountability and reliability of the distributed access control system in cloud federations	The scheme is time consuming for large data operations.
Privacy Preserving Access Control Protocol in Cloud Federations	This scheme gives better security by applying attribute based policies in terms of access control..	The scheme is not able to handle amounts of data accessed by the user
Fine Grained Access control Scheme Based on Cloud Storage	This method achieves user revocation along with reducing time for data owner to manage data. It realizes data sharing and data storage.	The efficiency is little slower.

6. PROPOSED METHODOLOGY

Various different schemes are available in the cloud environment to provide access control capability to the users. This enables the users to define access control policies so that only the authorized and authenticated users should be able to access the required data. But with the available schemes, comes a lot of issues of complexity, speed and overheads. To handle these issues, a new and improved methodology should be designed to be used in public cloud storage. So, here we proposed an “Efficient and Improved Scheme for Access Control and Secure Data Sharing in Public Cloud”. This schemes works as follows : The data and the information is shared by the users in the public cloud. Then the AES(Advanced Encryption Standard) algorithm is applied. This is the cryptographic algorithm to be used to give better security. This is one of the fastest encryption algorithm to encrypt the data and it is used in symmetric key cryptography. Then the privacy preserving data processing scheme is applied to help realize seven different operations on the encrypted data. This helps to perform easy computations on the encrypted data. Then at last the Role based Access control approach is used for restricting system access to authorized users. The roles are assigned to the particular subjects so that they can perform their functions. This RBAC can implement both the MAC(Mandatory Access Control) and DAC(Discretionary Access Control) policies. Thus the data now reaches the end user or the other users can securely access the data with access control rights defined to them.

The algorithm which is given below defines the flow of the proposed scheme :

Basic steps of algorithm:

Step 1: The user shares the data in the public cloud to be used by other users.

Step 2: Then the contents of data are encrypted using the AES algorithm to give faster encryption. This is used to secure the sensitive information.

Step 3: Then the privacy preserving data processing scheme is applied that enables to perform several different operations on the encrypted data.

Step 4: The Role Based Access Control approach is used to determine the access control rights assigned to a particular subject.

Step 5: The other users in the public cloud get access to the required data while having the access control rights defined to them.

Diagrammatic representation of proposed method is shown as follows:

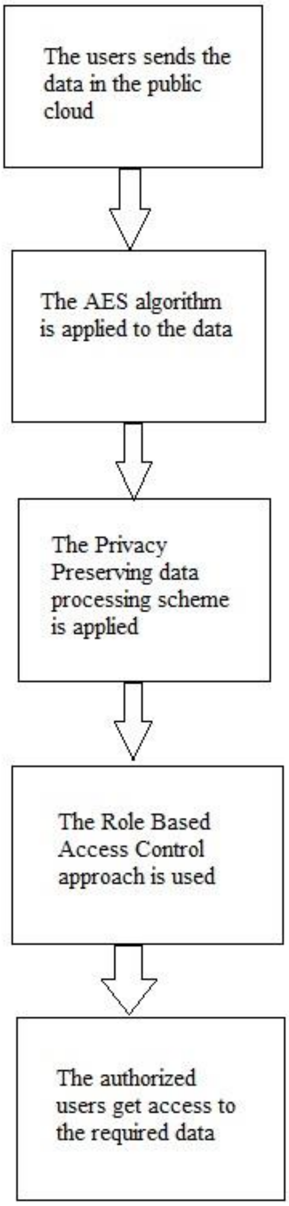
The users sends the data in the public cloud
The AES algorithm is applied to the data
The Privacy Preserving data processing scheme is applied
The Role Based Access Control approach is used
The authorized users get access to the required data

Fig 1: Flow of the Algorithm showing the proposed scheme

7. OUTCOME AND POSSIBLE RESULTS

In this way, the proposed scheme provides an efficient approach for sharing data in the public cloud storage while determining the access control rights to each user. The AES algorithm used provides for secure and faster encryption of the data. The privacy preserving scheme allows to perform seven different operations on the encrypted data and the RBAC determines access control rights for each user. Thus this methodology allows for accessing data securely in the public cloud and giving improved access control capability.

8. CONCLUSION

This paper focused on the study of different methods available for access control and secure data sharing in cloud. These schemes are : Privacy Preserving Data Processing with Flexible Access Control, Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage(RAAC), Decentralized Runtime Monitoring for Access Control Systems in Cloud Federations, Privacy Preserving Access Control Protocol in Cloud Federations, Fine Grained Access Control scheme. But these schemes have certain limitations in it. So to overcome those we have proposed an

"Efficient and Improved Scheme for Access Control and Secure Data Sharing in Public Cloud". It ables to determine the access control rights for the users so that the information is accessed only by the authorized users. This helps to securely share the sensitive data with the other users in the public cloud environment.

9. FUTURE SCOPE

From the observations of the proposed scheme, we can further implement it with more improved functions and lower overheads in it.

ACKNOWLEDGEMENT

This technical paper is supported by all the teaching and non-teaching staff of our department. I convey my sincere gratitude to Prof. Y. M. Kurwade. Without this kind direction and proper guidance this work would not have been possible. I also express my immense gratitude to V.M. Thakare for his continued support and encouragement along with suggestions which helped to improve the contents of this paper.

REFERENCES

[1] Wenxiu Ding, Zheng Yan, Robert H. Deng "Privacy Preserving Data Processing with Flexible Access Control", *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING* , 2017.

[2] Kaiping Xue, Yingjie Xue, Jianan Hong, Wei Li, Hao Yue, David S.L. Wei, Peilin Hong "RAAC: Robust and Auditable Access Control With Multipli Attribute Authorities for Public Cloud Storage", *IEEE TRANSCTIONS ON INFORMATION FORENSICS AND SECURITY"*, Vol. 12, No. 4, April 2017.

[3] Md. Sadek Ferdous, Andrea Margheri, Fedrica Paci, Mu Ynag, Vladimiro Sassone "Decentralized Runtime Monitoring for Access Control Systems in Cloud Federations", *IEEE International Conference on Distributed Systems*, 2017.

[4] Shorouq Alansari, Federica Paci, Andrea Margheri, Vladimiro Sassone "Privacy Preserving Access Control in Cloud Federations", *IEEE International Conference on Cloud Computing"*, 2017.

[5] Xiaojie Niu "Fine-grained Access Control Scheme Based on Cloud Storage", *IEEE International Conference on Computer network, Electronic and Automation*, 2017.

Author's profile:

	Shrutika P. Marke has completed B.E. Degree in Information technology from Sant Gadge Baba Amravati University, Amravati, Maharashtra. She is persuing Master's Degree in Computer Science and Information Technology from P.G. Department of Computer Science and Engineering, S.G.B.A.U. Amravati. (e-mail id: shrutimarke04@gmail.com)
	Yogeshwar M. Kurwade is Assistant Professor in the Department of Computer Science, Sant Gadge Baba Amravati University, Amravati. He is B.E(I.T) and completed his M.E(CSE). He has also cracked the GATE, NET and SET examinations. He has also published various papers in International & National level Journals and also International Conferences and National level Conferences. (e-mail id: yogeshwarkurwade@gmail.com)
	Vilas M. Thakare is Professor and Head in Post Graduate department of Computer Science and Engg, Faculty of Engineering & Technology, SGB Amravati university, Amravati. He is also working as a coordinator on UGC sponsored scheme of e-learning and m-learning specially designed for teaching and research. He is Ph.D. in Computer Science/Engg and completed M.E. in year 1989. He has done his PhD in area of robotics, AI and computer architecture. His area of research is Computer Architectures, AI and IT. He has published more than 150 papers in International & National level Journals and also International Conferences and National level Conferences. (e-mail id: vilthakare@yahoo.co.in)