International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com
ISSN No: 2456 - 6470 | Volume - 2 | Issue – 6 | Sep – Oct 2018

Some Studies on Protection for the Hidden Attribute Based Signatures without Anonymity Revocation

S. Mahathi[1], M. Ravindar[2]
[1]M.Tech Student, [2]Associate Professor
Department of Computer Science & Engineering,
Jyothishmathi Institute of Technology & Science, Karimnagar, Telangana, India

ABSTRACT
The purpose of this paper is to study of access control scheme to protect users' privacy in cloud environment is of great significance. In this paper, we present an access control system with privilege separation based on privacy protection. In the PS-ACS scheme, we divide the users into personal domain and public domain logically. In the PSD, we set read and write access permissions for users respectively. The Key-Aggregate Encryption is exploited to implement the read access permission which improves the access efficiency. A high degree of patient privacy is guaranteed simultaneously by exploiting an Improved Attribute-based Signature which can determine the users' write access. For the users of PUD, a hierarchical attribute-based encryption is applied to avoid the issues of single point of failure and complicated key distribution. Function and performance testing result shows that the PS-ACS scheme can achieve privacy protection in cloud based services.

Keywords: *Cloud, privacy protection, Signatures, Revocation.*

1. INTRODUCTION
Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties[1,3]. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme. We propose a novel access control system called PSACS, which is privilege separation based on privacy protection. The system uses Key-Aggregate Encryption scheme and Hierarchy Attribute-based Encryption scheme to implement read access control scheme in the PSD and PUD respectively. The KAE scheme greatly improves access efficiency and the HABE scheme largely reduces the task of a single authority and protects the privacy of user data.

2. LITERATURE SURVEY

A critical literature review of recent advances in development of Privacy Protection based Access Control Scheme in Cloud-based Services is presented in Table 1.

Table 1: Privacy Protection based Access Control Scheme in Cloud-based Service

Year	Author	Title	Important findings
2010	Shucheng Yu et.al.	Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing	In this paper authors presented the how To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. They achieved by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Authors presented scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that their proposed scheme is highly efficient and provably secure under existing security models.
2011	Sonia Jahid et.al.	Easier: Encryption-based Access Control in Social Networks with Efficient Revocation	In this paper, the authors discussed about the promising approach to mitigate the privacy risks in Online Social Networks (OSNs) is to shift access control enforcement from the OSN provider to the user by means of encryption. They proposed EASiER, an architecture that supports fine-grained access control policies and dynamic group membership by using attribute-based encryption. A key feature of their architecture is that it is possible to remove access from a user without issuing new keys to other users or re-encrypting existing cipher texts. They achieved this by creating a proxy that participates in the decryption process and enforces revocation constraints. The proxy is minimally trusted and cannot decrypt cipher texts or provide access to previously revoked users. Authors described EASiER architecture and construction; provide performance evaluation, and prototype application of our approach on Facebook.
2011	S E Wang and B G Lin	A Scheme Of Attribute-Based Encryption Access Policy Used In Mobile Cloud Storage For Personal Health Records	In this paper authors were investigated on how to solve the problem of efficiency and security existing in accessing control to personal health records (PHRs) through mobile client in the environment of Cloud Storage and also forwarded a scheme for mobile applications' access policy of PHRs under a semi-trusted server framework through using attribute-based encryption (ABE) and focusing on the multiple security domains scenario in this paper. Simulation experimental analysis also done. Finally investigators concluded that they can't determine that lazy re-encryption is the safest and most efficient algorithm and our

			access control policy is more outstanding than others.
2014	Mahesh B et.al.	Cloud Based PHR System for Privacy Preserving Using Attribute Based Encryption	In this paper authors presented the Attribute Based Encryption (ABE) technique for the personal health records stored in the semi-trusted servers. ABE is used to enable fine-grained and scalable access control for PHRs. To reduce the key distribution complexity, we divide the system into private and public domains. Thus, every patient can fully control their record. They also presented about the cloud server, records are stored using encryption technique which ensures the patient's full control over their PHR. The third party servers are semi trusted servers and hence it is important to provide encryption before outsource the PHR to the third party servers.
2016	Ragesh and Baskaran	Cryptographically Enforced Data Access Control in Personal Health Record Systems	The author discussed various aspects on how To deal with data security and privacy problems in cloud assisted PHR systems, various data access control schemes etc. In this paper proposes a revocable multi authority attribute set based encryption scheme to address the attribute revocation problem in multi authority cloud assisted PHR systems. They concluded the efficiency of the proposed scheme is greatly improved by updating the Components associated with the revoked attribute of the cipher text, while the other components which are not related to the revoked attribute are not changed. They also concluded their multi authority scheme achieves not only fine-grained data access control but also user revocation. Furthermore this scheme provides system flexibility and scalability along with forward and backward security.
2017	Aashruthaand D Sujatha	A Survey on Cross-License Cloud Storage Environment of Revelatory, Proficient, and Versatile Data Access Management	Authors were discussed about the economical and unstable data way administer proposal for multi-jurisdiction muddle storehouse systems, station skillful are numerous authorities synchronize and each law stand consequence associates severally. Specifically, they concentrated on a shifting multi-force CP-ABE blueprint and affect it as the basic techniques to form the data way manage blueprint. The also discussed about the trace repudiation method can competently reach both dispatch confidence and late freedom. They finally concluded that their proposed data entry command scenario is insure in the aimless divination represent and is more potent than earlier works. Authors were also presented the detailed review on available literature on proposed work.
2017	Zhang et.al.	PTBI: An efficient privacy-	This paper deals with the Biometric identification

		preserving biometric identification based on perturbed term in the cloud Author links open overlay panel	and its important role in achieving user authentication. The author also presented the For efficiency and economic savings, biometric data owners are motivated to outsource the biometric data and identification tasks to a third party, which however introduces potential threats to user's privacy. In this paper, they proposed a new privacy-preserving biometric identification scheme which can release the database owner from heavy computation burden. In the proposed scheme, their design concreted biometric data encryption and matching algorithms, and introduce perturb terms in each biometric data. A thorough analysis indicates that our schemes are secure, and the ultimate scheme offers a high level of privacy protection. In addition, the performance evaluations via extensive simulations demonstrate their schemes' efficiency.
2017	Chuan et.al.	PPDP:An efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system	This paper deals with Disease prediction systems which has played an important role in people's life, since predicting the risk of diseases is essential for people to lead a healthy life. The recent proliferation of data mining techniques has given rise to disease prediction systems. Specifically, with the vast amount of medical data generated every day, Single-Layer Perceptron can be utilized to obtain valuable information to construct a disease prediction system. Although the disease prediction system is quite promising, many challenges may limit it in practical use, including information security and prediction efficiency. In this paper, we propose an efficient and privacy-preserving disease prediction system, called PPDP. In PPDP, patients' historical medical data are encrypted and outsourced to the cloud server, which can be further utilized to train prediction models by using Single-Layer Perceptron learning algorithm in a privacy-preserving way. The risk of diseases for new coming medical data can be computed based on the prediction models.
2018	Supriya et.al.	Attribute Based Access Control in Personal Health Records Using Cloud Computing	In this paper authors investigated some important aspects of Personal health records (PHR) Associate in Nursing rising health data exchange model,that facilitates PHR homeowners to expeditiously share their personal health knowledge among a spread of users as well as attention professionals still as family and friends. In projected system Associate in Nursing attribute based mostly authorization mechanism wont to authorize access requesting users to access a given PHR resource supported the associated access policy whereas utilizing a proxy re-encryption theme to facilitate the approved users

			to decode the specified PHR files.
2018	Wencheng Sun et.al.	Security and Privacy in the Medical Internet of Things: A Review	In this paper the authors described about the Medical Internet of Things, also well known as MIoT, and also discussed on how it plays a more and more important role in improving the health, safety, and care of billions of people after its showing up. Instead of going to the hospital for help, patients' health-related parameters can be monitored remotely, continuously, and in real time, then processed, and transferred to medical data center, such as cloud storage, which greatly increases the efficiency, convenience, and cost performance of healthcare. The amount of data handled by MIoT devices grows exponentially, which means higher exposure of sensitive data. The security and privacy of the data collected from MIoT devices, either during their transmission to a cloud or while stored in a cloud, are major unsolved concerns. This paper focuses on the security and privacy requirements related to data flow in MIoT. In addition, they presented in-depth study on the existing solutions to security and privacy issues, together with the open challenges and research issues for future work [10].
2018	Dong et.al.	Cloud-based radio frequency identification authentication protocol with location privacy protection	In this present study, the author presented the security and privacy issues of the cloud-based radio frequency identification system are more serious than traditional radio frequency identification systems. The link between the reader and the cloud is no longer secure, and the cloud service provider is not trusted. Both the location privacy of the reader and the data privacy of the radio frequency identification system are not able to be exposed to the cloud service provider. In this article, a cloud-based radio frequency identification authentication protocol is proposed. It considers not only the mutual authentication between the reader and the tag, but also the security of data transmission between the reader and the cloud database [11]. In particular, in order to solve the reader's location privacy problem, the proposed scheme introduces MIPv6 network framework without adding additional infrastructure. The experimental verification with AVISPA tool shows that the protocol satisfies the mutual authentication property. Compared with other cloud-based schemes, the proposed protocol has obvious advantages in deployment cost, scalability, real-time authentication, and the tag's computational complexity.

3. SYSTEM ARCHITECTURE

The first and foremost strategy for development of a project starts from the thought of designing a mail enabled platform for a small firm in which it is easy and convenient of sending and receiving messages, there is a search engine ,address book and also including some entertaining games(Figure.1.). When it is approved by the organization and our project guide the first activity, ie. Preliminary investigation begins. The activity has three parts:

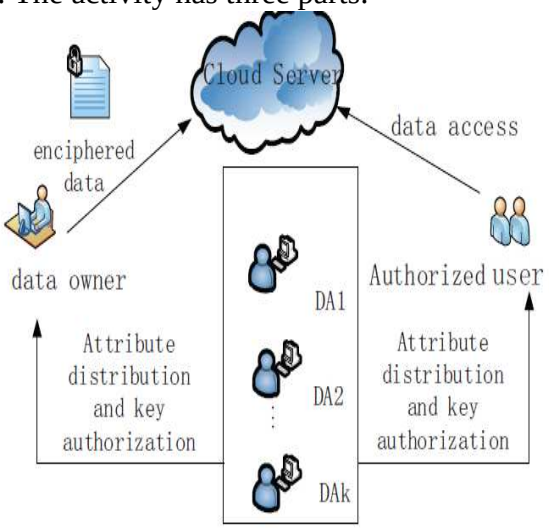

Figure.1.Proposed System architecture

- Request Clarification
- Feasibility Study
- Request Approval

3.1 Request Clarification

After the approval of the request to the organization and project guide, with an investigation being considered, the project request must be examined to determine precisely what the system requires[4,5]. Here our project is basically meant for users within the company whose systems can be interconnected by the Local Area Network (LAN). In today's busy schedule man need everything should be provided in a readymade manner. So taking into consideration of the vastly use of the net in day to day life, the corresponding development of the portal came into existence.

3.2 Feasibility Analysis

An important outcome of preliminary investigation is the determination that the system request is feasible [5].

3.3 Request Approval

Not all request projects are desirable or feasible. Some organization receives so many project requests from client users that only few of them are pursued. However, those projects that are both feasible and desirable should be put into schedule. After a project request is approved, it cost, priority, completion time and personnel requirement is estimated and used to determine where to add it to any project list[7,9]. Truly speaking, the approval of those above factors, development works can be launched.

CONCLUSION

In this paper, we propose access control system (PS-ACS), which is privilege separation based on privacy protection. Through the analysis of cloud environment and the characteristics of the user, we divide the users into personal domain (PSD) and public domain (PUD) logically. In the PSD, the KAE algorithm is applied to implement users read access permissions and greatly improved efficiency. The IABS scheme is employed to achieve the write permissions and the separation of read and write permissions to protect the privacy of the user's identity. In the PUD, we use the HABE scheme to avoid the issues of single point of failure and to achieve data sharing. Furthermore, the paper analyzes the scheme from security and efficiency, and the simulation results are given. By comparing with the MAH-ABE scheme, the proposed scheme shows the feasibility and superiority to protect the privacy of data in cloud-based services.

REFERENCES

1. S. Yu, C. Wang, K. Ren, "Achieving secure, scalable, and fine-graineddata access control in cloud computing," Proc. IEEE INFOCOM, pp. 1-9, 2010.
2. J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-basedencryption," Proc. Security and Privacy, pp. 321-334, 2007.
3. J. Hur, D. K. Noh, "Attribute-based access control with efficientrevocation in data outsourcing systems," IEEE Transactions on Paralleland Distributed Systems, vol. 22, no. 7 pp. 1214-1221, 2011.
4. A. Lewko, B. Waters, "Decentralizing attribute-Based encryption," Proc.Advances in Cryptology-EUROCRYPT, pp. 568-588, 2011.
5. M. Li, S. Yu, Y. Zheng, "Scalable and secure sharing of personal healthrecords in cloud computing using attribute-Based Encryption," IEEETransactions on Parallel and Distributed System, vol. 24, no. 1, pp. 131-143, 2013.

6. C. K. Chu, S. S. M. Chow, W. G. Tzeng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, 2014.

7. J. Li, K. Kim, "Hidden attribute-based signatures without anonymity revocation," Information Sciences, vol. 180, no. 9, pp. 1681-1689, 2010.

8. H. K. Maji, M. Prabhakaran, M. Rosulek, "Attribute-Based Signatures,"Proc. Topics in Cryptology - CT-RSA, pp. 376-392, 2011.

9. S. Kumar, S. Agrawal, S. Balaraman, "Attribute based signatures for bounded multi-level threshold circuits," Proc. Public Key Infrastructures, Services and Applications, pp. 141-154, 2011.

10. Dong, Qingkuan, et al. "Cloud-based radio frequency identification authentication protocol with location privacy protection." International Journal of Distributed Sensor Networks 14.1 (2018): 1550147718754969.

11. Sun, Wencheng, et al. "Security and privacy in the medical Internet of Things: A review." Security and Communication Networks 2018 (2018).

12. Karthik, Guntha, and Singam Jayanthu. "Review on low-cost wireless communication systems for slope stability monitoring in opencast mines." International Journal of Mining and Mineral Engineering 9.1 (2018): 21-31.