ENHANCED FEATURE BASED ATTRIBUTE ENCRYPTION FOR DATA PRIVACY AND ACCESS CONTROL

[1]Somireddy Pavani, [2]Dr.Arun Sahayadhas
[1]Research Scholar of Computer Science and Engineering, VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai
[2]Professor of Computer Science and Engineering, VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai
somi.phd@velsuniv.ac.in, arun.se@velsuniv.ac.in

ABSTRACT: The healthcare organization gathers a lot of complicated healthcare data that is not mined to get the confidential data needed to make wise decisions. The concept of personal health records has emerged as a patient-centered healthcare service where the patient's health data is gathered in the cloud. It provides the ability for people to produce, manage, and distribute data over the cloud. However, doing so necessitates taking security and privacy concerns into account. This work describes Enhanced Feature based Attribute Encryption for Data Privacy and Access Control, which is presented as a solution to these onerous commitments. Use an adaptable and fine-grained access control system to manage massive amounts of data. On unreliable servers, the ability to obtain and manipulate the entry with fine-grained information is guaranteed. In these techniques, it is up to the data owners to encrypt their files before uploading or downloading them to the cloud and to re-encrypt them if a client's login information changes. The outcomes demonstrate the efficiency and reliability of the approach to data access as well as sharing in the cloud computing. Access control comparison and computation cost comparison of various models are described in the result analysis. By outsourcing the procedure, the method will reduce the computing cost for consumers.

KEYWORDS: Feature Based Attribute Encryption, access control, data privacy, fine grained Authentication.

I. INTRODUCTION

Flexible access control strategies are needed for modern data outsourcing systems [1]. It is often preferable to offer differentiated access services so that user features or roles are used to set data access regulations.

A trusted server is responsible for setting and implementing access control regulations in classic access control systems like reference monitor. This method is challenged by the data outsourcing paradigm. Because users desire the ability to create an access policy and impose it on the contents, as well as share confidential content with a set of people they choose, modern data outsourcing technologies no longer operate under this presumption [2]. Consequently, it is preferable to provide data owners control over access policy decisions.

The providing of high services at reasonable prices is among the most difficult problems facing the healthcare industry (hospitals, medical facilities) [3]. The level of service reflects how well patients are diagnosed and how well they receive effective treatment. Poor clinical decision-making can have disastrous results that are unacceptable. The cost of clinical tests must also be decreased by hospitals. They can achieve these outcomes by using the proper computer-based information and/or decision support tools. Users and owners utilizing the Physical Health Records (PHR) service are multiplying immensely as the use of cloud computing rises tremendously [4].

Access control policies are determined by various aspects of the requester, environment, or data item in newly presented access control methods like attribute-based access control [5]. Additionally, present phenomenon of

eISSN 1303-5150

storage outsourcing necessitates greater data protection, including access control techniques with cryptographical enforcement. A promising strategy that satisfies these conditions is the invention of Attribute-Based Encryption (ABE). ABE has a method that allows access policies and assigned properties between private keys and ciphertexts to be used to control access to encrypted material. In particular, Ciphertext-Policy ABE (CP-ABE) provides a scalable data encryption approach in which encryptor specifies the collection of properties that the decryptor must possess to decrypt the ciphertext [6]. According to security policy, certain users are therefore permitted to decode various pieces of data. As a result of this, it is no longer necessary to depend on the storage server to stop illegal data access.

Encrypting the data prior to outsourcing would be a workable and viable strategy. In essence, Encryption methods and who may access each file should be decided by the PHR owner. PHR files ought to be kept private and only accessible to people who have been provided the necessary decryption keys [7]. Additionally, access privileges can always be granted and revoked by the patient as they see it necessary. But sustainability in a PHR system frequently clashes with the objective of patient-centric privacy. Either for personal or professional usage, the PHR may need to be accessed by the authenticated persons.

Some disease predictions are not automated. Public key encryption-based techniques were initially employed to encrypt the data from personal health records. However, the encryption was one-way and there was a lot of key management work required. A solution for effective key management and encryption is described despite this one-way approach, such as ABE (also called feature-based encryption), which is a one-to-many encryption methodology. It was described that the data may be encrypted using a set of qualities that would allow many users to decrypt the encrypted data using the provided key. The distinguishing feature of attribute-based encryption is that it stops multiple users from cooperating.

The system's significant features include, discovery of PHR record done by the revoked customers collaborating with current users in these approaches, it concentrate on developing an ABE method with effective client revocation for cloud infrastructure and furthermore, this approach would minimize significant computation cost for users. The methods can be applied to fine-grained enhanced attribute access control in cloud storage systems that needs client revocation capabilities [8]. With a diverse range of customers, including relatives, friends, professionals, specialists, and security offices, now, a user can have accessibility to his medical records in an appropriate manner.

II. LITERATURE SURVEY

Y. Zhang, D. Zheng, and R. H. Deng, et al. [9] developed privacy-aware s-health access control framework, where a broad universe CP-ABE with partially disguised access principles is suggested. The ciphertext size and decryption time cost of ABE systems grow together with the size of the access policy, which creates a problem.

Zheng Yan, Mingjun Wang, Yuxiang Li, Athanasios V. Vasilakos, et. al. [10] presents a method based on ABE to allow safe data access control and de-duplicate encrypted information stored in cloud. Employment rate for storage facilities, particularly for massive data, is significantly reduced by the possibility of storing duplicated data that is encrypted using various encryption algorithms on the cloud. Recently, a number of data de-duplication strategies have been suggested. The performance of the scheme is assessed by the authors through analysis and

eISSN 1303-5150

implementation. Results demonstrate the scheme's scalability, effectiveness, and efficiency for prospective adoption in practice.

Zheng Yan, Xueyun Li, Mingjun wang and Athanasios V. Vasilakos, et. al. [11] gives a way to manage flexible data access in the cloud computing utilizing ABE and proxy re-encryption based on the data owner's assessment of trust and/or reputations built by a number of reputation centers. It integrates the concept of context-aware trust as well as reputation evaluation into a cryptographic system in order to accommodate various control scenarios and approaches. Through in-depth research, security proof, comparison, and application, the performance and security of the method are assessed and justified. The outcomes describe, adaptability, effectiveness and efficiency of data access control approach for cloud computing.

J. H. Seo and K. Emura, et. al. [12] shown that the Identity-Based Encryption (IBE) prior revocation techniques are susceptible to decryption key disclosure. Revocable Identity-Based Signatures (RIBS) are reviewed from perspectives of security methods and structures. Initially, it shows that all earlier RIBE constructions, excluding the Boneh-Franklin one, are vulnerable to the legitimate threat known as decryption key disclosure. Second, it combines (adaptively secure) Waters IBE scheme and the (selectively secure) Boneh-Boyen IBE method to create first scalable RIBE approach with resistance to decryption key exposure. Then it demonstrate that RIBE approaches is highly effective than remaining prior flexibly secure scalable RIBE approaches. In order to demonstrate the viability of the solutions, it present implementation outcomes.

K. Yang and X. Jia, et. al. [13] presents, a dynamic auditing system that is effective and secure for cloud computing data storage. In the beginning, it develops a cloud storage system auditing architecture and suggests a successful and confidential auditing protocol. Then, because data dynamic operations are effective and secure in the random oracle paradigm, it modifies the auditing guidelines to support them. Without the aid of a reliable organizer, it further expand the auditing guidelines to accommodate auditing batch for the numerous owners and multiple clouds. Analysis as well as simulation findings demonstrate that presented auditing methods are effective, secure, particularly in lowering the auditor's computing costs.

M. Bellare, S. Keelveedhi, and T. Ristenpart, et al. [14] Message-Locked Encryption (MLE), an unique encryption technique, was presented to achieve deduplication of the encrypted data. Clients must encrypt their data using the object data's hash value in MLE-based schemes to guarantee that distinct clients can access the same encrypted copies of the identical plaintext information.

L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, et al. [15] The data server's semi-trusted proxy is used to offer CP-ABE schemes that provide quick attribute revocation instead of periodic or planned revocation. However, they have also failed to implement fine-grained user access control in context of data outsourcing.

N. Attrapadung and H. Imai, et. al. [16] suggested another user-revocable ABE strategies integrating broadcast encryption systems and ABE methods to overcome the issue. This solution requires the data owner to completely assume responsibility for managing all membership lists for each attribute group in order to permit direct user revocation. This plan cannot be used with the architecture for data outsourcing because, after data owners have outsourced their data to an external data server, they

eISSN 1303-5150

will no longer have direct control over how the data is distributed.

III. ENHANCED FEATURE BASED ATTRIBUTE ENCRYPTION

The overview of the architecture system of Enhanced Feature Based Attribute Encryption (FBAE) for Data Privacy and Access Control is represented in below Fig. 1

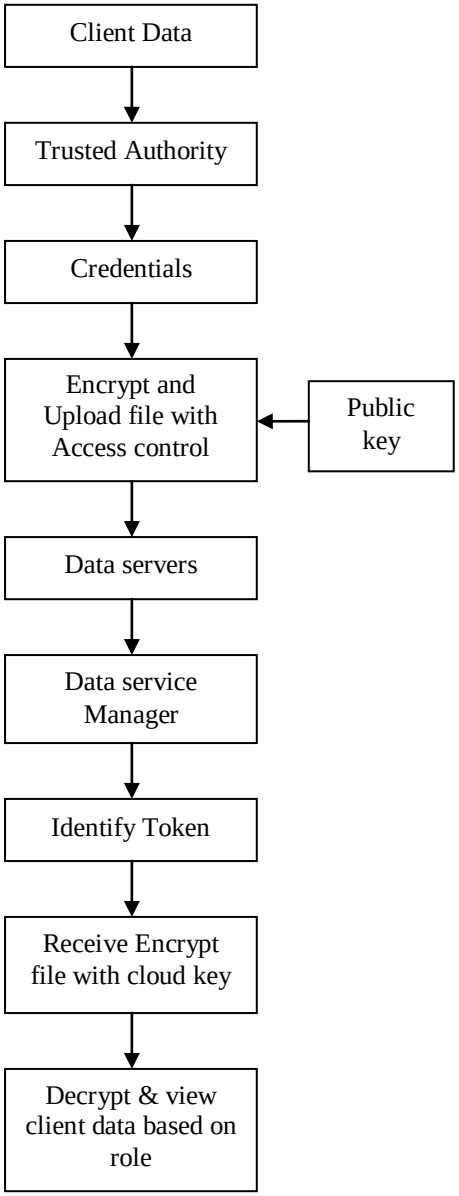

Fig. 1: OVERVIEW OF THE ARCHITECTURE SYSTEM

Attribute encryption based on features is dependent on a specific cryptography scheme. Customers receive their high-quality private keys provided by a property professional in particular in an FBAE plot. If the mark is significant, the endorser's qualities will be demonstrated to the verifier as satisfying the marking predicate. Cryptography system is quite well-known with open keys for access. Intervening cryptography involves using an online middleman for each exchange. Recently, Security Mediated Certificate (SMC) cryptography was also modified to represent property-based version of the Scanning Electron Microscope (SEM) cryptography. These various PHR access holders and clients use the PHR application process. The definition of a public health record owner is someone who has ownership over the patient data in a PHR. Each patient's PHR record is accessible to the PHR owner because they are deemed authorized users in order to carry out PHR sharing.

An important authority for the set of qualities is a respected source. It creates both open and closed variables for system. Giving users attribute keys and updating them as necessary are its responsibilities. Depending on their attributes, it gives each user a varied set of access permissions. All of the entities using the data outsourcing system completely rely on this one party.

A customer that has information and wants to transfer it to an exterior data server offered by service provider is referred to as a data owner. By encrypting the information covered by the policy before sending it to a third party, a data owner can enforce (attribute-based) access policy on its data. A client is an entity that requests access to the data that has been outsourced. If users possess a group of characteristics that fulfill the access policy established by data owner for such encrypted data and are not revoked in either of attribute groups, they will be permitted to decrypt the ciphertext and obtain the data. Before uploading or

eISSN 1303-5150

downloading data to or from the cloud, the data owners are responsible for encrypting it. They are also responsible for re-encrypting the data if a client's login information changes.

One who offers data outsourcing services is referred to as a service provider. A data service manager and data servers make up this system. Data servers are used to store data that data owners have outsourced. Data service manager is responsible for controlling external users' access to the servers that host the outsourced information and offering the necessary contents solutions. It takes the data service manager's curiosity and honesty into account, just like the earlier schemes. This means that it will faithfully carry out the tasks that have been delegated by proper system participants. It would nevertheless wish to understand as much as it can about encrypted contents. The management of each attribute group's attribute group keys is under the responsibility of the data service manager.

Attribute groups G_j for every $\lambda_j \in \Lambda$ to the data service manager is given by the trusted authority. For instance, if u_1, u_2, u_3 are related to $\{\lambda_1, \lambda_2, \lambda_3\}$,$\{\lambda_2, \lambda_3\}$, $\{\lambda_1, \lambda_3\}$, respectively, trusted authority gives $G_1 = \{u_1, u_3\}$, $G_2 = \{u_1, u_2\}$, $G_3 = \{u_1, u_2, u_3\}$ to data service manager.

Key Encrypting Key (KEK) Generation: Data service manager will then execute KEKGen(U) and then produce KEKs for customers in U. Data service manager first creates binary KEK tree to user universe μ, that is utilized to assign keys of attribute group to members in U⊆ μ. In tree, every node v_j of tree contains KEK, indicated by the KEK_j. Path keys are collection of KEKs on nodes that form the path from a leaf to the root. The following phase involves identifying various tokens or properties.

The attribute group key is decrypted form the header Hdr during the data decryption step, after which the message decryption from CT' (encrypted CipherText Whenever user obtains ciphertext (Hdr, CT') by data service manager, He initially acquires keys for each attribute group in Λ held by user from a Hdr. If a user u_t contains viable attribute λ_j (that is, $u_t \in G_j$), it decrypt attribute group key K_{λ_j} by Hdr utilizing KEK which is normal in $KEK\ (G_j)$ and $PK_t\ (t\square at\ is, KEK\ \in\ KEK\ (G_j) \cap$ $\mathcal{PKt}$. Due to the fact that there can only be one such KEK, the user can only be a member of one subset that is rooted by one KEK in KEK (G_j).

The following Revoking Attribute updates were done in MA-FBAE (Multiple user Access FBAE).

- Public key components have been changed for impacted attribute.
- Elements that are upgraded in a secret key to reflect each client's revoked status.

Additionally changed on that server was the Cipher text attribute.

In this way, the framework has advantages that are entirely silent driven by extremely strict limited management and it strengthens security assurance.

IV. RESULT ANALYSIS

In this part, it examines the presented scheme's effectiveness in terms of access control granularity. The efficiency of suggested scheme is then analyzed and contrasted with that of the earlier CP-ABE strategies in terms of theory. In the network simulation, the described scheme's effectiveness is shown in terms of communication costs. It also discuss about how effective it is when used with certain parameters and contrast the outcomes with those of the other systems.

eISSN 1303-5150

The level of access control granularity and rekeying for each method are shown in Table 1. In the suggested approach, the data service manager rather than CP-ABE can perform the rekeying right away. As a result, a user or an attribute may be removed at any moment, even before any possible attribute expiration period. By closing the windows of susceptibility that permit unwanted access to the data, this increases the backward and forward secrecy of the outsourced data's confidentiality. The suggested system also implements more precise user access control for every attribute.

Table 1: ACCESS CONTROL COMPARISON

Used model	Access Control Granularity	Rekeying
CP-ABE	Attribute revocation	Timed rekeying
CP-ABE with efficient Revocation	System level user revocation	Immediate rekeying
FBAE	Attribute level user revocation	Immediate rekeying

Fig. 2 compares the cost of calculation for various levels of privacy derived models as CP-ABE with efficient Revocation, CP-ABE and Feature based Attribute Encryption. As can be shown, the CP-ABE technique uses 210.645 ms and 232.869 ms, respectively, when there are 400 and 1000 files. The computation time for CP-ABE along with effective Revocation for the same number of files is 26.029 ms and 25.987 ms, respectively. FBAE for Data Privacy and Access Control model, which is more effective than other models, uses 10.012 milliseconds and 9.011 milliseconds, respectively, almost a negligible constant.

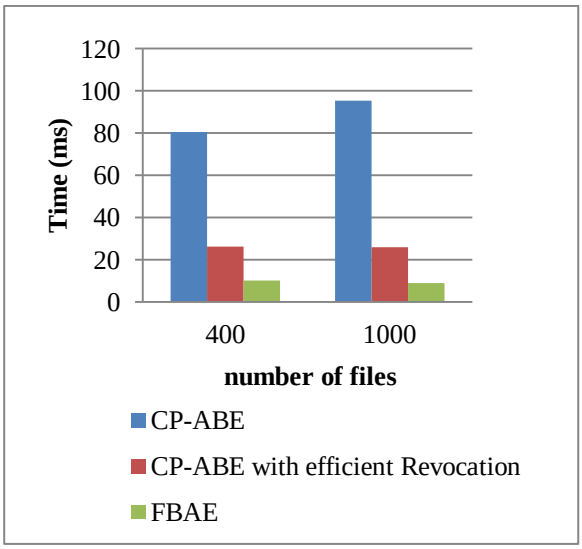

Fig. 2: THE COMPARISON OF COMPUTATION COST FOR DIFFERENT MODELS

V. CONCLUSION

In this paper, Enhanced FBAE for Data Privacy and Access Control is described. The PHR is a crucial health-related management system for keeping someone's health information safe. In order to create a safe information sharing system, these data are kept on unreliable servers. The presented technique allows a data owner to define the access control policy as well as apply it to outsourced data. On untrusted servers, the ability to access and manipulate fine-grained information is guaranteed. Additionally, it has a method with effective attribute and user revocation capabilities that provides more precise access control. Access control comparison and computation cost comparison of various models are described in the result analysis. The outcomes demonstrate how efficient and successful the approach is for gaining access and sharing data in the cloud.

VI. REFERENCES

[1] Sultan Badran, Nabil Arman, Mousa Farajallah, “An Efficient Approach for Secure data outsourcing using Hybrid data Partitioning”, 2021 International Conference on Information Technology (ICIT), Year: 2021

eISSN 1303-5150

[2] Qinlong Huang, Yixian Yang, Wei Yue, Yue He, "Secure data Group Sharing and Conditional Dissemination with Multi-owner in Cloud Computing", IEEE Transactions on Cloud Computing, Year: 2021
[3] Mohini Bhardwaj, Nitin Pandey, Vinod Kumar Shukla, Ajay Vikram Singh, Neetu Gupta, "Review and Analysis of Security Model in health care System", 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Year: 2021
[4] S. Kanaga Suba Raja, A. Sathya, L. Priya, "A Hybrid data Access Control Using AES and RSA for Ensuring Privacy in Electronic Healthcare Records", 2020 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Year: 2020
[5] Rohit Ahuja, Sraban Kumar Mohanty, "A Scalable attribute based access control Scheme with Flexible Delegation cum Sharing of access Privileges for Cloud Storage", IEEE Transactions on Cloud Computing, Volume: 8, Issue: 1, Year: 2020
[6] Guangli Xiang, Beilei Li, Xiannong Fu, Mengsen Xia,Weiyi Ke, "An Attribute Revocable CP-ABE Schem", 2019 Seventh International Conference on Advanced Cloud and Big Data (CBD), Year: 2019
[7] Alex Roehrs, Cristiano André da Costa, Rodrigo da Rosa Righi, Sandro José Rigo, Matheus Henrique Wichman, "Toward a Model for Personal Health record Interoperability",IEEE Journal of Biomedical and Health Informatics, Year: 2019
[8] Wei Li, Bonnie M. Liu, Dongxi Liu, Ren Ping Liu, Peishun Wang, Shoushan Luo, Wei Ni, "Unified Fine-Grained Access Control for Personal Health records in Cloud Computing", IEEE Journal of Biomedical and Health Informatics, Volume: 23, Issue: 3, Year: 2019
[9] Y. Zhang, D. Zheng, and R. H. Deng, ''Security and privacy in smart health: Efficient policy-hiding attribute-based access control,'' IEEE Internet Things J., vol. 5, no. 3, pp. 2130–2145, Jun. 2018.
[10] Zheng Yan, Mingjun Wang, Yuxiang Li, Athanasios V. Vasilakos, "Encrypted Data Management with Deduplication in Cloud Computing", IEEE Cloud Computing, Volume: 3, Issue: 2, Year: 2016
[11] Zheng Yan, Xueyun Li, Mingjun wang and Athanasios V. Vasilakos, "Flexible Data Access Control based on Trust and Reputation in Cloud Computing" 2015, IEEE transactions on cloud Computing, DOI 10.1109/TCC 2015.2469662.
[12] J. H. Seo and K. Emura, ''Revocable identity-based cryptosystem revisited: Security models and constructions,'' IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1193–1205, Jul. 2014.
[13] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in Cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013
[14] M. Bellare, S. Keelveedhi, and T. Ristenpart, ''Message-locked encryption and secure deduplication,'' in Proc. IACR Cryptol. ePrint Archive, P. Q. Nguyen, Ed., 2012, pp. 296–312.
[15] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application," Proc. Int'l Workshop Information Security Applications (WISA '09), pp. 309-323, 2009.
[16] N. Attrapadung and H. Imai, "Conjunctive Broadcast and Attribute-Based Encryption," Pairing '09: Proc. Int'l Conf. Palo Alto on Pairing-Based Cryptography, pp. 248-265, 2009.