A Survey on Hierarchical Attribute Set Based Encryption Access Control Method for Mobile Cloud Computing

G.Narmadhai[1], Dr. S. Vijay Bhanu[2]
[1, 2] Dept of Computer Science
[1, 2] Annamalai University Annamalai Nagar- 608 002.

Abstract- *Cloud Computing is going to be a very popular technology in IT enterprises. For any enterprise the data stored is very huge and invaluable, since all tasks are performed through network, it has become vital to have the secured use of genuine data. In cloud computing the most important matter of concern are data security and privacy along with flexibility, scalability and fine-grained access control of data are the other requirements to be maintained by cloud systems. Access control is one of the well-known research topics and hence various schemes have been proposed and implemented. But most of them do not present flexibility, scalability and fine-grained access control of the data on the cloud. In order to address the issues of flexibility, scalability and fine-grained access control of distantly stored data on cloud the proposed scheme uses modified hierarchical attribute set-based encryption (MHASBE) which is the extension of hierarchical attribute- set-based encryption (HASBE) with a hierarchical structure of users. The proposed scheme achieves scalability by handling the authority to suitable entity in the hierarchical structure, inherits flexibility by allowing easy transfer and access to the data in case of location switch. It provides fine-grained access control of data by showing only the requested and authorized details to the user thus improving the performance of the system. In addition, it provides competent user revocation within expiration time, request to view extra-attributes and privacy in the intra-level hierarchy. This scheme is implemented to demonstrate that it is efficient in access control of data as well as security of data stored on cloud with complete experiments performed.*

Keywords- Fine-grained access control; attribute-set-based encryption(ASBE); hierarchical attribute-set-based encryption(HASBE); user revocation; intra-level hierarchy

I. INTRODUCTION

Cloud computing is rising computing technology that uses on the Internet. It consists of the use of computing resources that are delivered as a service over a network. In cloud computing model users have to give access to their data for storing and performing the preferred business operations. Hence cloud service provider(CSP) must provide the trust and security, as there is valuable and sensitive data in enormous amount stored in the clouds. There are concerns about flexible, scalable and fine grained access control in the cloud computing. For this purpose, there have been many of the schemes, proposed for encryption. Such as a simple encryption technique that is typically studied. Here we are going to discuss about the Attribute-Based Encryption (ABE) schemes and how it has been developed and modified further into Key Policy Attribute based encryption (KP-ABE). Cipher-text Policy Attribute Based Encryption (CP-ABE) and further, it has been proposed as CP-ASBE and furthermore HABE and HASBE so on. This is according to how flexible, scalable and fine grained access control is provided by each scheme. Cloud computing has rapidly become a widely adopted paradigm for delivering services over the internet. Therefore cloud service provider (CSP) must provide the trust and security, as there is valuable and sensitive data in large amount of data stored on the clouds. For protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud by using some cryptographic algorithms. Here in this paper, we are going to discuss about attribute based encryption scheme and its categories. With the growing of network technology and mobile terminals, meanwhile, cloud computing is one of the most promising application platforms to solve the volatile expanding of data sharing. In cloud computing, to protect data from data leakages, users need to encrypt their data before being shared. Access control is supreme as it is the first line of defense that prevents unauthorized access to the shared data. Recently, Attribute-Based Encryption (ABE) has been attracting much more attention since it can keep data privacy and realize fine-grained, one-to-many, and non interactive access control. Ciphertext-policy attribute based encryption (CP-ABE) is one of feasible schemes which has much more flexibility and is more suitable for general applications authority accepts the user enrollment and creates some parameters. A cloud service provider (CSP) is the manager of cloud servers and provides

multiple services for client. Data owner encrypts and uploads the generated ciphertext to CSP. User downloads and decrypts the interested ciphertext from CSP. The shared files usually have a hierarchical structure. That is, a group of files is divided into a number of hierarchy subgroups located at different access levels. If the files in the same hierarchical structure could be encrypted by an integrated access structure, the storage cost of ciphertext and time cost of encryption could be saved. A patient divides his PHR information M into two parts: personal information m1 that may contain the patient's name, social security number, telephone number, home address, etc. The medical record m2 which does not contain sensitive personal information, such as medical test results, treatment protocols, and operation notes. Then the patient adopts CP-ABE scheme to encrypt the information m1 and m2 by different access policies based on the actual need. For example, an attending physician needs to access both the patient's name and his medical record in order to make a diagnosis, and medical researcher only needs to access some medical test results for academic purpose in the related area, where a doctor must be a medical researcher, and the converse is not necessarily true. Meanwhile, access structure could be shared by the two files. Therefore, the computation complexity of encryption and storage overhead of the ciphertext can be reduced greatly. Moreover, since transport nodes are added to the access structure, users can decrypt all authorization files with computation of secret key once. The computation cost of decryption can also be reduced if users need to decrypt multiple files at the same time.

II. REVIEW OF LITERATURE

Shulan Wang and their friends finds [1] revisit attribute-based data sharing scheme in order to solve the key escrow issues, but also improve the expressiveness of attribute, so that the resulting scheme is friendlier to cloud computing applications. They proposed an improved two-party key issuing protocol that can guarantee that neither key ability nor the cloud service provider can compromise the entire secret key of a user individually. Moreover, they introduce the concept of attribute with weight, being provided to enhance the expression of attributes, which can not only expand the expression from binary to arbitrary state, but also lighten the complexity of access policy. Therefore, both storage cost and the encryption complexity for a cipher text are relieved.

Sahai and Waters introduced an attribute based encryption scheme by [6] the goal is to provide security and access control shows that how to decrease a communication overhead between cloud server and data owner using public key compression technique for fully homomorphic encryption scheme over the integers. Whenever we use the cloud, user expects data privacy, search accuracy and less communication overhead from the cloud service providers. In order tackle this TRSE (Two Round Searchable Encryption) scheme has been proposed which achieved high data privacy through homomorphic encryption and search accuracy through vector space model. The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it uses the access of monotonic attributes to control user's access in the system.

Vipul et al. discovered an attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. Which states that as more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). A new cryptosystem is developed for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In the cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is capable to decrypt. It demonstrates the applicability of the construction to sharing of audit-log information and broadcast encryption. The construction supports allocation of private keys which subsume Hierarchical Identity-Based Encryption (HIBE).

Rakesh et al. discovered—Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption elaborates that in distributed systems users need to share sensitive objects with others base on the recipients ability to satisfy a policy. Attribute- Based Encryption (ABE) is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. Ciphertext-Policy ABE (CP-ABE) is a form of ABE where policies are associated with encrypted data and attributes are associated with keys. In this work focus is on improving the flexibility of representing user attributes with keys. Specifically, it proposes the Ciphertext Policy Attribute Set Based Encryption (CP-ASBE) - a new form of CP-ABE- which, unlike existing CP-ABE schemes that represent user attributes as a monolithic set in keys, organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. It shows that the proposed scheme is more versatile and supports many practical scenarios more naturally and efficiently. It provides a prototype implementation of the scheme and evaluates its performance overhead.

Pankaj et al. find out the Cloud Computing Security Issues in Infrastructure as a Service explains that cloud computing promises to cut operational and capital costs and the additional important thing is it lets IT departments focus on planned projects instead of keeping datacenters running. It is much more than simple internet. It is a build that allows user to access applications that is in fact reside at location other than users own computer or other Internet connected devices. There are many benefits of this construct. For example other company hosts user application. This implies that they handle cost of servers, they manage software updates and depending on the contract user pays less i.e. for the service only. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer will certainly affect the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. It presents an elaborated study of IaaS components security and determines vulnerabilities and countermeasures. Service Level Agreement(SLA) should be considered very much importance.

John et al. —Ciphertext-Policy Attribute-Based Encryption (CP-ABE) explains that in several distributed systems a user should only be able to access data if a user possesses a confident set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using this technique encrypted data can be kept confidential even if the storage server is untrusted; moreover, the methods are secure against conspiracy attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into users keys; while in this system attributes are used to describe the users credentials, and a party encrypting data determines a policy for who can decrypt. Thus, these methods are theoretically closer to traditional access control methods such as Role-Based Access Control(RBAC). In addition, it provides an implementation of system and gives performance measurements.

Suhair et al. discussed the designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption, which shows that as more and more healthcare organizations adopt electronic health records (EHRs), the case for cloud data storage becomes forceful for deploying EHR systems; not only is it reasonably priced but it also provides the flexible, wide-area mobile access increasingly needed in the modern world. However, before cloud-based EHR systems can become a reality, issues of data security, patient privacy, and overall performance must be addressed. As standard encryption (including symmetric key and public-key) techniques for EHR encryption/decryption caused increased access control and performance overhead, the scheme proposes the use of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to encrypt EHRs based on healthcare providers' attributes or credentials; to decrypt EHRs, they must possess the set of attributes needed for proper access. It motivates and presents the design and usage of a cloud based EHR system based on CP-ABE, along with preliminary experiments and analysis to investigate the flexibility and scalability of the proposed approach.

Ayad and their research colleague discusses Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage System, which proposes a cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has four important features: (i) it allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion and append the data, (ii) it ensures that authorized users (i.e., those who have the right to access the owners file) receive the latest version of the outsourced data, (iii) it enables not direct mutual trust between the owner and the CSP, and (iv) it allows the owner to grant or rescind access to the outsourced data. The security issues of the proposed scheme are discussed. Besides, it justifies its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overheads.

Patrick et al. discovered the methods and limitations of security policy reconciliation, which explains that a security policy is a means by which participant session requirements are specified. However, existing frameworks provide limited amenities for the automated understanding of participant policies. It considers the limits and methods of reconciliation in a general-purpose policy model. It identifies an algorithm for well-organized two-policy reconciliation, and show that, in the worst-case, reconciliation of three or more policies is intractable. Further, it suggests efficient heuristics for the detection and resolution of intractable reconciliation. Based upon the policy model, it describes the design and implementation of the Ismene policy language. The expressiveness of Ismene, and indirectly of the model, is demonstrated through the representation and exposition of policies supported by existing policy languages. It concludes with brief notes on the integration and enforcement of Ismene policy within the Antigone.

Guojun et al. published their work ―Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, which explains that with fast development of cloud computing, more and more enterprises will outsource their susceptible data for sharing in a cloud. To keep the shared data confidential against untrusted cloud service providers (CSPs), a usual way is to store only the encrypted data in a cloud. The key problems of this approach include establishing access control for the encrypted data and revoking the access rights from users when they are no longer authorized to access the encrypted data. It aims to solve both problems. First, it proposes a hierarchical attribute-based encryption scheme (HABE) by combining a hierarchical identity-based encryption (HIBE) system and a Ciphertext policy attribute-based encryption(CP-ABE) system, so as to provide not only fine-grained access control, but also full allocation and high performance. Then, it proposes a scalable revocation scheme by applying proxy re-encryption (PRE) and lazy re-encryption (LRE) to the HABE scheme, so as to efficiently revoke access rights from users.

Kaitai Liang and Willy Susilo proposed a novel[3]searchable attribute-based proxy re-encryption system. When compared to existing systems only supporting either searchable attribute based functionality or attribute-based proxy re-encryption, this new primitive support both abilities and provides flexible key word update service. Specifically, the system enables a data owner to efficiently share their data to a specified group of users matching a sharing policy and meanwhile, the data will maintain its searchable property but also the corresponding search keyword(s) can be updated after the data sharing. The server, however knows nothing about the keyword(s) and the data. The new mechanism is appropriate to many real-world applications, such as electronic health record systems.

Y. Zheng proposed Expressive Key-Policy ABE, the encryption methods in clouds Attribute-based encryption (ABE), allows fine grained access control on encrypted data. In the key policy attribute based encryption, the primitive enables senders to encrypt messages with a set of attributes and private keys are associated with access tree structure that specifies which all the ciphertexts the key holder is allowed to decrypt. In most ABE systems, the ciphertext size grows linearly with the number of ciphertext attributes and the only known exceptions only support restricted forms of threshold access policies. This expressive key-policy attribute based encryption (KP-ABE) schemes allowing for non-monotonic access and with constant ciphertext size. The private keys have quadratic size in the number of attributes. On the other hand, they reduce the number of pairing evaluation size to a constant, which appears to be a unique feature among expressive KP-ABE schemes. This is more efficient than KPABE.

Waters et.al, proposed *"Fuzzy-Identity Based Encryption"* concept that permits error-tolerance within private key and public key which is used for cipher text encryption. Here mainly to two applications of F-IBE scheme used are ABE and biometrics. It hides the general public key that was want to encipher the cipher-text is intriguing. It is simplified version of Bilinear Diffie Hellman Decisional assumption. It motivates few open problems that is creating attributes from different authorities, uses distance metrics within identities.

In **Kan Yang et.al.** Proposed a revocable multi-authority CP-ABE scheme, to resolve the attribute revocation problem in the system. The attribute revocation method can professionally achieve both forward security and backward security. Furthermore, while updating the cipher texts, all the users need to hold only the most recent secret key, rather than to keep records on all the previous secret keys. But this system issues computation efficiency and the revocation method.

A.B. Lewko et.al. presented two fully secured functional encryption schemes: a fully secure attribute based encryption(ABE) scheme and a fully secure (attribute hiding) predicate encryption (PE) scheme for inner product predicates. They constructed their ABE scheme in composite order bilinear groups, and prove its security from three static assumptions. Their ABE scheme supports arbitrary monotone access formulas. Their predicate encryption scheme is constructed via a new approach on bilinear pairings using the notion of dual pairing vector spaces projected by Okamoto and Takashima.

A.B. Lewko et.al. proposed a fully decentralized ABE where users could have zero or more attributes from each authority and did not require a trusted server. In all these cases, decryption at user's end is computation intensive. So, this technique might be inefficient when users access using their mobile devices.

S. Ruj et.al used technique that requires owners to re-encrypt the cipertext. The method in need owner to generate the update information during the revocation, where the owner should also hold the encryption secret for ciphertext in the system. This incurred a heavy storage overhead on the owner, especially when the number of ciphertext is large in the cloud storage system. Hence there is need of a better scheme for data access controls in the cloud storage were the cloud servers are not trustworthy.

Sahai and Waters put forward a new encryption mechanism which uses the attribute set to encrypt the data [3] and the

main goal of the system was to provide security and access control. The mentioned scheme has four algorithms: i)Setup, ii)Encryption, iii)Key generation and iv)Decryption. The setup phase a random input is given to the algorithm to get the Master key as well as public parameters as output. In the encryption phase the set of attribute is taken as input along with the outputs from the first phase to generate the encrypted message. In the key generation phase, it outputs a key for the decryption phase, and in the final stage, i.e., the decryption phase the original message is retrieved from the cipher text by using the decryption key. Collusion resistance is one of the crucial security features of the ABE system. If one user has multiple keys then one of the keys should be matched in-order to grant access to data. The disadvantage of the ABE scheme is that the data owner needs to use every authorized public key to encrypt data. The application of the scheme is restricted in the real environment since it uses the access of monotonic attributes to control user's access in the system.

Bettencourt, Sahai and Waters [3] proposed two methods that are derived from attribute based encryption based on the difference in the deployment. Both works with the same algorithms as in the case of attribute based encryption. The algorithm has four phases as explained in the previous method, i.e., Setup, Encryption, Key Generation and Decryption. The key policy based attribute based encryption scheme can achieve fine grained access control and flexibility than ABE. The drawback with the scheme is that the encrypt or cannot decide who can decrypt the encrypted data. The same is inappropriate for some application as the data owner need to trust the key issuer. In the case of cipher text policy based attribute based encryption, the scheme overcomes the drawbacks of KP-ABE i.e., the encrypted data could choose who can decrypt. The user's private key is a combination of a set of attributes. The flaws of the existing CP-ABE schemes are not fulfilling the enterprise requirements of the access control that need efficiency and flexibility. In CP-ABE decryption keys only support user attributes that are organized logically as a single set so that users could use all the possible combinations of the same. The CP-ASBE consists of recursive sets of attributes. There is challenge for preventing users from combining attributes from multiple keys.

R. Ostrovsky and B. Waters [7] proposed another ABE scheme with non-monotonic access structure. They can use negative words to define each attribute in the message, whereas the monotonic access structure cannot. The mentioned scheme being ABE works as same as the classical ABE scheme consisting of the four algorithms. Being non monotonic ABE the encryption phase as well as the decryption phase are slightly different from that of the classical ABE. In the encryption phase, rather than taking the access structure as input the algorithm takes non-monotonic access structure as input and in the decryption phase, the plain text is derived from the cipher text based on the same non-monotonic access structure. The problem with the ABE scheme over non-monotonic access structures is that there are many negative attributes in the encrypted data. It can reason the encrypted data overhead to huge. It is inefficient and compound that each cipher text needs to be encrypted with d attributes, d is a system-wise constant.

Wang et al.[8] proposed the hierarchical attribute based encryption in which it uses the property of a hierarchical generation of keys. Also, it can be used to achieve proxy re-encryption[4]. Proxy re-encryption schemes are the cryptosystems that are used to alter the cipher text that has been encrypted by one user so that the same could be decrypted by another user. The method employs two algorithms instead of key generation. The algorithms are Setup, Create domain masters, Create users, Encryption and Decryption. But the same is impractical to implement. As all of the attributes in one conjunctive clause in this scheme may be managed by the same domain authority, the same attribute may be managed by multiple domain authorities.

V Bozovic, D Socek, R Steinwandt, and Vil-lanyi [2] proposed Multi-Authority Attribute Based Encryption in which the scheme employs the following algorithms. Setup, Attribute Key Generation, Central key generation, Encryption and Decryption. The setup algorithm is a randomized algorithm run by a third party and it gives a master key as output. In the attribute key generation phase the secret key is generated as output taking the users' GID, the authority's value dk and a set of attributes in the authority's domain and the randomized algorithm is run by the attribute authority. The algorithm in the next phase is run by the central authority central key generation. The algorithm gives the secret key for the user as the output taking the master key as well as user's GID as input. The encryption phase runs as same as that of in the traditional ABE and is run by the sender. The decryption algorithm is a deterministic algorithm run by the user. Takes as input decryption keys for an attribute set Au and a cipher text, which was encrypted under attribute set AC. Outputs a message m if $|Ak\ C \cap Ak\ u| > dk$ for all authorities k. Complication in multi-authority scheme requires that the authority's attribute set be disjoint.

III. SUMMARY OF LITERATURE REVIEW

Table 1.1 Summary of Literature Review

S.No	Parameters vs. ABE techniques	Author	Year	Fine-Grained Access Control	Efficiency
1.	KP-ABE(Key Policy Attribute based encryption)	V. Goyal, O., Pandey, A.,Sahai, and B.Waters	2006	Low	Average
2.	EKP-ABE (Expressive Key Policy Attribute Based	S. Yu, C. Wang, K. Ren, and W. Lou	2010	Better Access control than that of KP-ABE	Higher than KP-ABE, Allows constant cipher text
3.	CP-ABE (Ciphertext Policy Attribute Based Encryption)	J. Bethencourt, A. Sahai, and B. Waters	2007	Average Realization of complex Access Control	Average Not efficient for modern enterprise environments
4.	CP-ASBE (Ciphertext Policy Attribute Set Based Encryption)	R. Bobba, H. Khurana, and M. Prabhakaran	2009	Better Access Control than that of CP-ABE	Better than CP-ABE as there is Less collusion attacks
5.	HIBE (Hierarchical Identity Based Encryption)	A. Sahai and B. Waters	2005	Lower than CP-ASBE	Better, Lower as compared to ABE schemes
6.	HASBE (Hierarchical Attribute Set Based Encryption)	Zhiguo Wan, Jun'e Liu, and Robert H. Deng	2012	Better Access control	Most efficient and flexible

IV. COMPARISON

The comparisons of above discuss Encryption techniques are shown in table-1.2.

Table 1.2- Comparison of Encryption Scheme.

Techniques	Access Control	Scalability	Efficiency	Flexibility	Security
ABE	High	High	Low	High	Low
KP-ABE	High	Low	Low	Low	Low
CP-ABE	High	Low	High	Low	Low
IBE	Low	Low	Low	Low	High
HABE	High	High	Low	Low	Low
DABE	Low	Low	High	Low	High
MA-ABE	High	High	High	High	Low

V. EXISTING SYSTEM

A hierarchical access control method using a hierarchical attribute-based encryption (HABE) and a modified three-layer structure is proposed. Differing from the existing paradigms such as the HABE algorithm and the original three-layer structure, the novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the application users with legal access authorities to get the corresponding sensed data and to confine illegal users and unauthorized legal users get access to the data, the proposed promising paradigm makes it extremely suitable for the mobile cloud computing based paradigm. What should be emphasized is that the most important highlight of all the proposed work can be described as that the modified three-layer structure is designed for solving the security issues illustrated.

VI. PROBLEM STATEMENT

Most deniable public key schemes are bitwise, which defines these methods can only practice one bit a time; thus, bitwise deniable encryption schemes are ineffective for real use, especially in the cloud storage service. To solve this problem, this paper planned a hybrid encryption scheme that parallel applies symmetric and asymmetric encryption. They utilize a deniably encrypted plan-ahead symmetric data encryption key, while real data are encrypted through a symmetric key encryption method. Most deniable encryption schemes have decryption error troubles. These errors arrive from the designed decryption mechanisms. It uses the subset decision mechanism for decryption. The receiver finds out the decrypted message according to the subset decision answer. If the sender chooses an aspect from the worldwide set, but unfortunately the element is located in the specific subset, then mistake occurs. The same error takes place in all translucent set-based deniable encryption schemes.

VII. PROPOSED SYSTEM

Those issues can be solved by providing methods of access control in the Cloud. Attribute Based Encryption (ABE) is a recent cryptographic primitive which has been used for access control. Access control issue deals with providing access to allow users and preventing unauthorized users to access data. Attaching a list of authorized users to each data is the simplest solution to attain access control. However, this solution is difficult in the scenario with a large number of users, such as the application mentioned above within the environment of cloud.

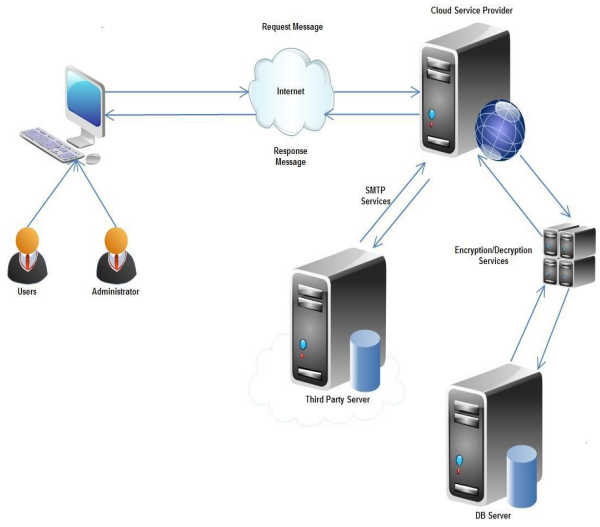

Fig. 1 System Architecture

Public cryptographic scheme is another solution, in which a public/secret key pair is given to each user and encrypt each message with the public key of the authorized user, so that only the specific users are able to decrypt it. In our proposed scenario, users with different privilege levels have different rights to access the part of sensing data coming from the mobile devices. Therefore, one similar data has to be encrypted into ciphertext once, which ought to be able to be decrypted multiple times by dissimilar authorized users.

Performance evaluation

There are different parameters to evaluate the performance of the existing attribute-based encryption methods in cloud computing as follows:

(1) Ciphertext size (communication cost): The size of file that the data owner has to send to the cloud service provider or the size of file that cloud service provider sends to users,
(2) Private key size (storage cost): It indicates the required storage for each user to store the private key,
(3) Public key size: It shows the required storage to store the public key of authorities in the ABE method,
(4) Re-keying size: It indicates the size of the rekeying message that can be used to recognize the user revocation for each attribute in the ABE system,
(5) Computation cost on the data owner: It indicates the required time to encrypt data by a data owner, and
(6) Computation cost on the user: It shows the required time to decrypt data by a user. Table 3 depicts the performance comparison of some of the existing method based on the aforementioned parameters.

VIII. CONCLUSION

The demand of PHR system in cloud computing is enormously increasing. So, the usage and dealing with cloud computing security preservation and cost estimation are in large quantities increasing as the need of the people is increasing day by day. To overcome those aspects the preferred security goals must be achieved. In this paper, the survey of different encryption schemes is mentioned with their advantage and disadvantage. The different variation of this scheme are compared and discussed with the existing scheme according to the rise in the security issues in cloud computing. The comparisons and study of those encryption scheme are done according to the problems arise and the solution on those the problem are mentioned. Theoretically, this survey paper thus introduced the various achievement and limitations that are or will take place in the cloud PHR system in future. Therefore for improving the security aspects the various concerns are made and the best approach is introduced to gain confidentiality to existing systems. The improvement in multi authority attributes encryption scheme is shown on removing the Central Authority. The three different existing of MAABE is discussed to be established more secure and which difficulties are handled on removing of CA and the solution to these difficulties is discussed shortly. Hopes this survey paper will help in estimating the differences in various encryption techniques to make the future improvements in further.

IX. ACKNOWLEDGMENT

We express our sincere thanks to all authors whose papers in the area of cloud computing are published in various conferences, proceedings and journals.

REFERENCES

[1] Shulan Wang, Kaitai Liang, Joseph K. Liu, Jianyong Chen, Jianping Yu, Weixin Xie ,"Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEE Transactions on Information Forensics and Security, 2016.
[2] Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu,Jianyong Chen, Weixin Xie ,"An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing", IEEE Transactions on Information Forensics and Security, 2016.
[3] Kaitai Liang and Willy Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage", IEEE Transactions on Information Forensics and Security, 2015
[4] JieXu, Qiaoyan Wen, Wenmin Li and Zhengping Jin,"Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing", IEEE TRANSACTIONS ON PARALLELAND DISTRIBUTED SYSTEMS ,2015
[5] Danwei Chen, Liangqing Wan, Chen Wang, Su Pan,YutingJi, "A Multi-authority Attribute-based Encryption Scheme with Pre-decryption", 2015 IEEE Seventh International Symposium on Parallel Architectures, Algorithms and Programming
[6] J. Bettencourt, A. Sahai, and B.Waters" Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.
[7] V Bozovic, D Socek, R Steinwandt, and V. I. Vil-lanyi, "Multiauthority attribute-based encryption with honest but-curious central authority" International Journal of Computer Mathematics, vol. 89,pp. 3,2012.
[8] V. Goyal, O. Pandey, A. Sahai, and B.Waters" Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM

conference on Computer and communications security, pp. 89{98, 2006}

[9] Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012.

[10] M. Pirretti, P. Traynor, P. Mc Daniel, and B. Waters. "Secure attribute-based systems". In Proceedings of the 13th ACM conference on Computer and communications security, pages 99{112. ACM Press NewYork, NY, USA, 2006

[11] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, ―Attribute- Sets: A Practically Motivated Enhancement to Attribute-Based Encryption‖, July 27, 2009 S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, ―A novel ultra thin elevated channel low-temperature poly-Si TFT,‖ IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, ―Achieving secure, scalable, and fine-grained data access control in cloud computing,‖ in Proc. IEEE INFOCOM 2010, 2010, pp. 534–542.

[13] J.Bethencourt, A. Sahai, and B. Waters. ―Ciphertext-Policy Attribute- Based Encryption.‖ In Proc. of SP'07, Washington, DC, USA, 2007.

[14] Zhibin Zhou, Dijiang Huang‖ On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption‖.

[15] R.Ostrovsky, A. Sahai, and B. Waters. ―Attribute-based encryption with non-monotonic access structures‖. In Proc. of CCS'06, New York, NY, 2007

[16] D.Boneh and M. Franklin. ―Identity-Based Encryption from the Weil Pairing.‖ In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.

[17] Guojun Wang, Qin Liu , Jie Wu ―Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud services‖, 2011.

[18] G.Wang, Q. Liu, and J.Wu, ―Hierachical attibute-based encryption for fine-grained access control in cloud storage services,‖ in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.

[19] P. D. McDaniel and A. Prakash, ―Methods and limitations of security policy reconciliation,‖ in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2002.

[20] A.Sahai and B. Waters. ―Fuzzy Identity-Based Encryption.‖ In Proc. Of EUROCRYPT'05, Aarhus, Denmark,
2005..

[21] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, ―HASBE:A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing‖ IEEE Transactions On Information Forensics And Security, Vol. 7, No.2,April2012.