International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 6, November - December 2015 ISSN 2278-6856

Certainty Based Privacy Service Mechanism on Key Policy Behavioral Based Encryption

Neha Mourya[1*], Margi Patel[2]

[1*] Research Scholar, Department of Computer & Science Engineering,
Oriental University, Indore (M. P.), India

[2]Assistant Professor, Department of Computer & Science Engineering,
Indore Institute of Science & Technology, Indore (M. P.), India

Abstract

Data storage on cloud is provided by the service provider. Storage of this data on un-trusted storage makes secure data sharing a challenging issue. Confidentiality of the data on this unknown environment can be achieved via various access control & encryption mechanism. Conventional encryption standards & techniques will only provide the basic things of security which can be breached. To achieve fine grained access control & effective data access control policies attribute based encryption is well defined standard [1]. There are various encryption algorithms available like AES, 3DES, blowfish etc. which will also provide the encryption based security but in a defined manner [2]. It is a burdensome of user to deal with their complex processes. For further improvements in existing methodology of security this work focuses on attribute based encryption with trust value. This work describe the basic utility of applying attribute based encryption (ABE) for data sharing on untrusted storage & servers. According to the specified problem the domain cloud security this work gives the solution to the mentioned security issues through CBPSM protocol stack in two steps. In first step, the user focuses on the revocation methodologies based on ABE. It gives the access control mechanism according to the user access historical details.

Keywords: CBPSM (Certainty Based Privacy Service Mechanism), ABE (Attribute Based Encryption), DES (Data encryption standard), Trust Model, etc.

1. INTRODUCTION

The proposed scheme of CBPSM hides the user's data own policy from itself & the server. In second step the scheme suggest the ABE based unique key generation for encryption & decryption for cloud storage. This key can be generated without the knowledge of accessing profile user & is done by selecting the random attributes from user table.

Attribute based encryption is also called as behavior based encryption (BBE). In this the cipher texts and user keys are associated with policies that describe the user that is allowed to access the encrypted information. Specifically, in Key-Policy ABE (KP-ABE) cipher texts are encrypted with a set of attributes and each user's secret key is associated with a policy describing which cipher texts user can decrypt.[2]

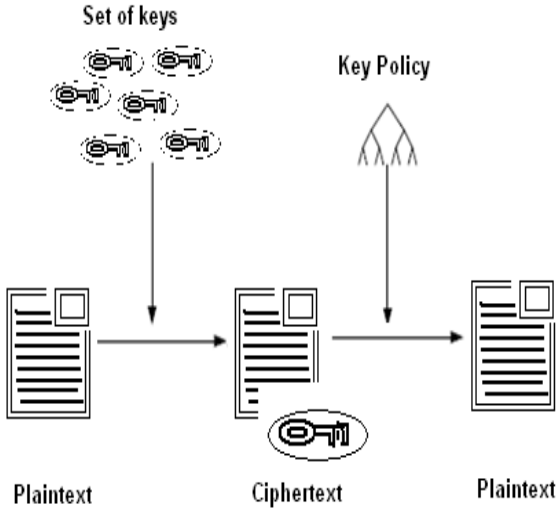

Figure 1:- Schematic diagram of KP-ABE

Conversely, in Cipher text Policy Attribute Based cryptography (CP-ABC) a cipher text is encrypted with a policy [14]. An attribute may be a property or feature that an issue might have. At some purpose in time, any subject might become eligible for a specific attribute, which means that it currently has the individual property or feature. It then receives a token from a trusty party referred to as attribute authority that testifies his eligibility and might be utilized by him to prove that he has the property or feature that the corresponding attribute represents. An attribute is typically delineated as a string. For example, an attribute called is Admin could be used to describe subjects that are administrators of a certain domain. We denote the set of all attributes used in a specific domain as the universe of attributes [3].

The attribute based encryption for generating the cipher texts is an extraordinary approach in which user profiles plays a vital role. It gives the access policies for encrypted information. These are mainly used to only generate the key attributes associated with each user & its type of data which it might be access every time. Key Generated Policy Attribute for Encryption (KGPAE) cipher texts are encrypted with a set of attributes and each user's secret key is associated with a policy describing which cipher text he can decrypt. Conventionally this can be achieved by taking the policy for encryption & then generates its

cipher values. Similarly anyone whose attributes satisfy the policy can decrypt the cipher texts; otherwise the decryption fails. An attribute is a property or feature that a subject may have. At some point in time, any subject may become eligible for a particular attribute, meaning that it now has the respective property or feature.

Types and Applications

As cloud applications is gaining popularity these days so as their applications also, like in healthcare, military, transportation, business intelligence, banking, and in information technologies applications. IT is the sector which is affected at most by these newer technologies and is proving magic tools in front of its customers.

These change n scenarios has come because of ABE's applicability over the various areas. Some of those properties is presented here as follows:

(i) **Flexibility:** ABE organizes user attributes into a recursive set structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. So ABE can support compound attributes and multiple numerical assignments for a given attribute conveniently.

(ii) **Fine-grained access control:** Based on ABE scheme can easily achieve fine-grained access control. A data owner can define and enforce expressive and flexible access policy for data files as the scheme.

(iii) **Efficient User Revocation:** To deal with user revocation in cloud computing, ABE adds an attribute to each user's key and employ multiple value assignments for this attribute. So we can update user's key by simply adding a new expiration value to the existing key. The approach just require a domain authority to maintain some state information of the user keys and avoid the need to generate and distribute new keys on a frequent basis, which makes our scheme more efficient than existing schemes.

(iv) Expressiveness: In ABE, a user's key is associated with a set of attributes, so ABE is conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). Thus, it is more natural to apply ABE, instead of KP-ABE, to enforce access control.

The main assistance of the projected work are as follows:

1. An evenly defined set of rules is required for outsourcing data policies for normal client to cloud platform.
2. The providers need not to be awake about the type of information or data stored on it. It will only be completed by some of the official user with right authorization.
3. An enhancement is made over a traditional ABE scheme, such that dependability over key generation is separated between a data holder and a trusted authority, the owner is comforted of the highest computational load.
4. Add-on security mechanism is provided through a combination of key mechanism using composite key generation.
5. Re-encryption is used as a method of transforming the stored cipher texts, permits efficient revocation of users; it does not require removal of attributes and consequent key regeneration, and may be administer by a trusted authority without participation of the data vendor.[4]

2. BACKGROUND

The primary concern of this work to make the things related to storage more secure without increasing the burden of operating user that is client. After applying the proposed protocol of CBPSM the client can be make the things sure about the security. The CBPSM will also focuses on the parameters of performance which gives the idea that while applying the model complexity can under a certain level. Secure computing environments require flexible access control method. For the big user category, access control policy for server cannot be individually based on entity user identities. The situation under which access needs to be given is based on client information like perspective, profile & earlier participation of the use or data. Because of these flaws of conventional access control mechanism, encryption mechanism are forced into this access policies & getting popularity. [5]

To make data in unreadable form uncountable approaches are advised by researches. Basically the method to make data unreadable form is named as encryption or cryptography. Cryptography or encryption algorithms act an important role in data security. Cloud computing provides highly scalable and more reliable storage on third-party trusted servers. It is reasonable pay-per-use utility model results in a reduction of the cost of deployment of the same computing resources locally. The key concern about cloud computing is data outsourcing to a cloud which is the storage of critical information related to clients system in third party servers at distributed locations. It is appropriate for any class of applications that requires data to be kept in storage and disseminated to many users. [6]

3. RELATED STUDY

Users that use cloud services will typically pay only for the amount of storage it uses and computation it performs and the network infrastructure in uses but it doesn't pay for the maintenance purpose. In additional to that it provides the secure storage capacity and data backups & recovery. But these data is stored at third party locations thus needs more trust on the cloud providers. A major concern that is typically not sufficiently addressed in practice which is [5]. The data stored at cloud locations may be accessed and read by a cloud administrator without knowledge of the client. A cloud administrator may not be trusted despite the presence of contractual security obligations, if data security is not further enforced through technical means. [7]

Therefore, it is useful to apply software techniques, such as encryption keys, to ensure that the confidentiality of cloud data is preserved at all times. It is especially crucial

to safeguard sensitive user data such as e-mails, personal customer information, financial records, and medical records. However, the main purpose of the access control based cryptography is not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation for cloud based data records [8]. Anonymous access control is a very desirable property in various applications, e.g. encrypted storage in distributed environments; and attribute based encryption is a cryptographic scheme that is targeted to achieve this property. ABE is an encryption mechanism that is useful in settings where the list of users may not be known prior. Here, all users may possess some credentials, and these are used to determine access control and also provide a reasonable degree of anonymity with respect to the user's identity. Due to these shortcomings of traditional access control mechanisms, cryptographically enforced access control receives increasing attention. [9]
The access control & better encryption standard one of the most promising approach can be used named as attribute based encryption through cipher text only policies. In this scheme, users possess sets of attributes (and corresponding secret attribute keys) that describe certain properties. Cipher texts are encrypted according to an access control policy, formulated as a Boolean formula over the attributes. The construction assures that only users whose attributes satisfy the access control policy are able to decrypt the cipher texts with their secret attribute keys [10]. The construction is required to satisfy a collusion resistance property: It must be impossible for several users to pool their attribute keys such that they are able to decrypt a cipher texts which they would not be able to decrypt individually. There are so many other transformation based schemes available like HNT Transformation [9], Bayes Network & HMM & hop by hop mechanism for authentication [11]. These above security & authentication mechanism can also be applied in various other domains like used in [12]. Cipher texts policy attribute based encryption is a scheme that gives a natural way to separate the credentials from the access policy and cleverly combine them at a later stage to provide secure access to protected data. In most ABE schemes the size of the cipher texts is quite large and is of the order of the number of attributes. In this work we present our approach for a multi-level threshold attribute based encryption which is independent of the number of attributes.

4. PROBLEM IDENTIFICATION

All through to storing the data or information at third place client or user not confident about the data stored safely. There are chances of unusual attacks all through the storage and retrieval of data to/from third location. Data may be tampered and accessed by legitimate user or external attacker. To make protection and sustain privacy its desires number of security mechanisms. So by verifying the formulations of trouble this can find the better outcome in case of both the types of attribute based encryption KP-ABE & CP-ABE. It wishes to keep in concern about the different objectives of information security on this un-trusted server of cloud & storage as given. The recommended dilemma has depict in this model

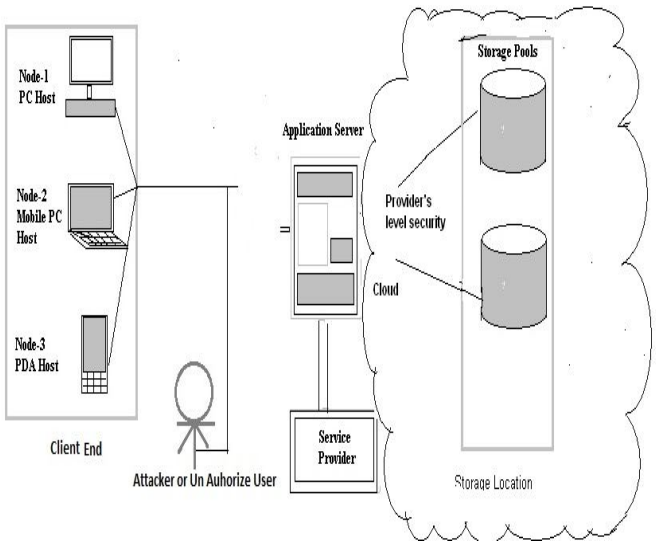

Figure 2:- Records Access by illicit User or invader

The above model shows a known dilemma that realized at client end during the retrieval and storing of information at cloud. Here may be any attacker or illegal person present to tamper or access the data ahead of data reach at client or cloud providers. Attacker may be influence client delicate or economic life so here need to avoid from this manner of activity require lot of techniques be used in data storage. To solve this problem one approach is also proposed by our-self to maintain data safe from unlawful access. Initially believe the server to be semi-trusted, i.e., honest but probing. That means the server will try to find out as much secret information in the stored record files as feasible, but they will sincerely follow the protocol in broad. At the few times users try to access the data beyond their boundary limits and privileges. To achieve this access area needs to be decided to avoid collision or isolation issues. Initially the work assumes that each user in our system is allotted some preventive public or private key pair. It is used for further enhancement in authentication of user area by user behavior or its attribute elements.
Thus to relate the ABE properly one wants to deal with all the dynamic attributes and keep informed the same as preferred. After knowing the different approaches that can be applied to deal with the dynamic attributes this work can make the subsequent are the least requirements of any vibrant attribute-updating scheme. For the work considers the server to be trusted, i.e., truthful but snooping. That way the server will attempt to find out a lot secret data in the stored record documents as achievable, but they will openly follow the protocol in common. On the other hand, some users will also try to access the files beyond their privileges. To do so, they may collude with other users, or even with the server. [13]

5. PROPOSED CBPSM APPROACH

Unauthorized access of data, cloud made unreliable for client. To provide reliability on cloud, an approach CBPSM is advised at client end to make safe and secure storage of data. The proposed approach is stack of multiple protections layer that deals with clients' data to providing overlapping layers of authentication, conviction analysis and make data unreadable form using conviction based encryption mechanisms. The suggested CBPSM approach consists of several phases.

Firstly to coated authentication layer to the data by providing identity of users and verifying the claimed identity. Secondly to coated conviction analysis layer to the data by regular observing the activities of users on the basis of historical property. Third phase is to coated conviction based encryption layer by converting client data into encrypted data and send for storage on the cloud. Figure 1 depicted suggested approach.

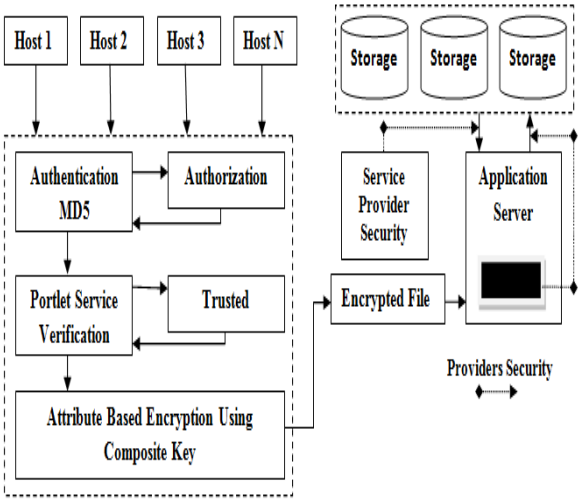

Figure 3:- CBPSM Security Using ABE

The CBPSM model shows stack of protection layer for the client data that are coated in different of phases such as Authentication of a separate decision related strictly to authorization. The separation of these three functions (Registration, Authentication and Authorization) by entrusting them to separate entities can be beneficial from a privacy enhancing perspective, as it links and restricts the permissible data processing actions and the availability of personal data to the specific tasks of each actor.

6. PERFORMANCE ASSESSMENT

The security and performance requirements are summarized as follows:

- **Information privacy.** Unauthorized users (including the server) who do not possess enough attributes satisfying the access policy or do not have proper key access privileges should be prevented from decrypting a record document, even under user collusion. Fine-grained access control should be enforced, meaning different users are authorized to read different sets of documents.
- **On-demand revocation.** Whenever a user's attribute is no longer valid, the user should not be able to access future record files using that attribute. This is usually called attribute revocation, and the corresponding security property is forward secrecy. There is also user revocation, where all of a user's access privileges are revoked.
- **Write access control.** We shall prevent the unauthorized contributors to gain write-access to owner's record, while the legitimate contributors should access the server with accountability. The data access policies should be flexible, i.e. dynamic changes to the predefined policies shall be allowed, and especially the records should be accessible under emergency scenarios.
- **Scalability, efficiency and usability.** The records system should support users from both the personal domain and public domains. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. Additionally, the owners' efforts in managing users and keys should be minimized to enjoy usability.

7. CONCLUSION

The proposed key based scheme has a new property that we can controlled user end security which is not known to be present (to the best of our knowledge) in any of the previous key based attribute signature schemes. This is a feature that would allow the user key to control their anonymity even if it well perform on any network whether is not determined by them or not. Let us say Alice is signing a document which wants a key to provide security, and she has sufficient attributes to satisfy the result. After studying the different approaches for providing the security against the outsourced environment of cloud computing this work had identified some the research objectives to work on for further improvements in existing mechanisms. [14]

8. FUTURE WORK

Taken security as a major concern in this work has generated so many integration issues. While applying the above proposed architecture component must be placed in correcting order for better results. The security breaches identification can be done as a real time entity. Behavior based encryption, access control, data isolation & key handling issues can also be improved effectively by using CBPSM model standard. Hence some problems and concepts that remain unaddressed can be performed. The implementation of the above proposed mechanism is configured in Java platform. [15]

9. ACKNOWLEDGEMENT

The authors wish to acknowledge Oriental University, Indore and Indore Institute of Science & Technology, Indore administration for their support & motivation during this research. The authors would also like to thank the anonymous referees for their many helpful comments, which have strengthened the paper. Many thanks to all the dignitaries for their discussions regarding the cloud

security policies & for producing the approach adapted for this paper.

REFERENCES

[1] Ming Li, Shucheng Yu, Yao Zheng, Student, Kui Ren, & Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption" in IEEE Transactions on Parallel & Distributed systems, 2012.

[2] Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish" in JGRCS, Volume 3, No. 8, August 2012.

[3] Deepak Garg, Limin Jia & Anupam Datta "Policy Auditing over Incomplete Logs: Theory, Implementation and Applications" in ACM 978-1-4503-0948-6/11/10 in 2011.

[4] Yanlin Li, Jonathan M. McCune, and Adrian Perrig, "VIPER: Verifying the Integrity of Peripherals' Firmware" in ACM 978-1-4503-0948-6/11/10 in 2011.

[5] Eric Y. Chen, Jason Bau & Charles Reis "App Isolation: Get the Security of Multiple Browsers with Just One" in ACM 978-1-4503-0948-6/11/10 in 2011.

[6] Jiyong Jang , David Brumley & Shobha Venkataraman in " BitShred: Feature Hashing Malware for Scalable Triage and Semantic

[7] Omar Elkeelan & Adegoke Olabisi, "Performance Comparisons, Design, and Implementation of RC5 Symmetric Encryption Core using Reconfigurable Hardware" in Acedmic Publisher, 2008.

[8] Sasirekha N, Hemalatha M , "An Enhanced Code Encryption Approach with HNT Transformations for Software Security", International Journal of Computer Applications (0975 – 8887) Volume 53– No.10, September 2012

[9] Nagaraju Devarakonda, Srinivasulu Pamidi, V Valli Kumari & A Govardhan, " Integrated Bayes Network and Hidden Markov Model for Host Based IDS" in IJCA Volume 41– No.20, March 2012.

[10] Maisam Mohammadian, Nasser Mozayani, "Improving of Authentication Mechanism in IMS Environment by Integration Hop By Hop and End To End Model", International Journal of Soft Computing and Software Engineering (JSCSE) e-ISSN: 2251-7545 Vol.2, 2012.

[11] Ziming Zhao & Gail-Joon Ahn, "Risk-Aware Mitigation for MANET Routing Attacks" in IEEE Transaction on dependable & secure computing, vol 9, No. 2, 2012.

[12] Rakesh Bobba, Himanshu Khurana & Manoj Prabhakaran, "Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption" in University of Illinois at Urbana-Champaign, July 2009.

[13] John Bethencourt, Amit Sahai & Brent Waters, "Cipher text – Policy Attribute-Based Encryption", in NSF CNS-0524252 US Army Research, in 2009.

[14] Kan Yang, Zhen Liu, Zhenfu Cao, Xiaohua Jia, Duncan S. Wong & Kui Ren, "TAAC: Temporal Attribute-based Access Control for Multi-Authority Cloud Storage Systems" in University at Buffalo, 2011.

AUTHOR

Neha Mourya received the Bachelors of Engineering in Information Technology from Shri Dadaji Institue of Technology & Science Khandwa (M. P.), India and she is a Research Scholar at Oriental University, Indore, India. Her major research areas are networking, distributed computing etc.

Margi Patel received the Bachelors of Engineering in Information Technology from J.I.T Borawan, Khargone and Masters of Engineering degrees in Computer & Science Engineering from IET DAVV University, Indore. Her Masters is in Software Engineering and major research areas are distributed computing, MANET, networking, etc.