International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 09
May 2016

An Enhanced Efficient User Revocation Mechanism with Anonymous Attribute Based Encryption

Pinjari Fakruddin[1]& H.Ateeq Ahmed[2]

[1] M.Tech Student, Department of CSE, Dr.K.V.Subba Reddy Institute of Technology
[2] Assistant Professor, Department of CSE, Dr.K.V.Subba Reddy Institute of Technology

Abstract:
Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper we show how AnonyControl-F extends the User Revocation algorithm with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control. Second, we demonstrate how to implement a full-fledged access control scheme for cloud computing. The scheme provides full support for hierarchical user grant, file creation, file deletion, and user revocation in cloud computing. Third, we formally prove the security of the proposed scheme based on the security Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against un-trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to un-trusted cloud servers without disclosing the underlying data contents.

1. INTRODUCTION

CLOUD Computing set up pervasive, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be immediately provision and released with essential efforts for management or service provider interaction. Its main objective is to deliver quick, secure , convenient data storage and net computing service, with all computing resources envision as services and delivered over the Internet.

A number of computing concepts and technologies are combined in Cloud Computing to satisfy the computing needs of users , it provides common business applications online through web browsers, while their data and software's are stored on the servers. This is an approach that is used to maximize the scope or step up capabilities robustly without investing in new infrastructure, sustenance new personnel or licensing new software. It provides tremendous storage for data and rapid computing to customers over the internet.

Data security is one of the aspects of the cloud which prohibit users from using cloud services. There is fear between the data owner's especially in large organizations that their data possibly misuse by the cloud provider without their

knowledge. Data security of the user's can be ensured by using the concept of virtual private networks, firewalls, and by enforcing other security policies within its own circumferences. Security is consequently an extensive element in any cloud computing environment, because it is crucial to assure that only authorized access is sanctioned and protected behavior Is accepted . Any kind of security and privacy contravention is critical and can produce crucial results. As soon as the strict regulations and policies are taken against privacy in cloud, more and more personnel will feel save to adopt cloud computing. A client may be individual or a big organization but all are having same concern i.e. data security, so data security is dire consequence. Data security at different levels is the vital matter of this technology; it can be categorized into two categories: Security at External level and Security at Internal Level.

Security at External level states that data is unsecure opposed to third party, cloud service provider or network intruder. Security at Internal level states that data is unsecure opposed To authorized users or employee of an organization. A secure server plus provides a protected foundation for hosting your Web applications, and Web server configuration plays a critical role in your Web application's security. Badly configured server can lead to unauthorized access. A forgotten share can provide a convenient back door, while an overlooked port can be an attacker's front door. Neglected user accounts can permit an attacker to slip by your defenses unnoticed Understanding threats to your Web server and being able to identify appropriate countermeasures permits you to anticipate many attacks and thwart the ever growing numbers of attackers. This system provides bidirectional encryption of communications between a client and server, which protects against eaves dropping and tampering with and/or forging the contents of the communication. In practice, this provides a reasonable guarantee that one is communicating with precisely. The website that one intended to communicate with, as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party.

Secure Server Plus application has mainly double login security. That is, after logging into the application user receives a secret key on his registered gmail id . This secret key has to be entered in the pop -up box displayed after logging into SSP Application. This application has two functionalities, Encryption and Decryption. Encryption is the functionality in which the file to be sent over mail in firstly divided into 4 equal parts in byte format and then encrypted using different encryption algorithms .After Encryption files would be sent to recipient through Gmail At the recipient end, He will download the files and using SSP Application data in files would be decrypted and merged.

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. Ciphertexts 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 ciphertexts 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 ciphertexts 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]. Ciphertexts 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 ciphertexts 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. PROPSED APPROACH

Attribute Authorities:
Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes.

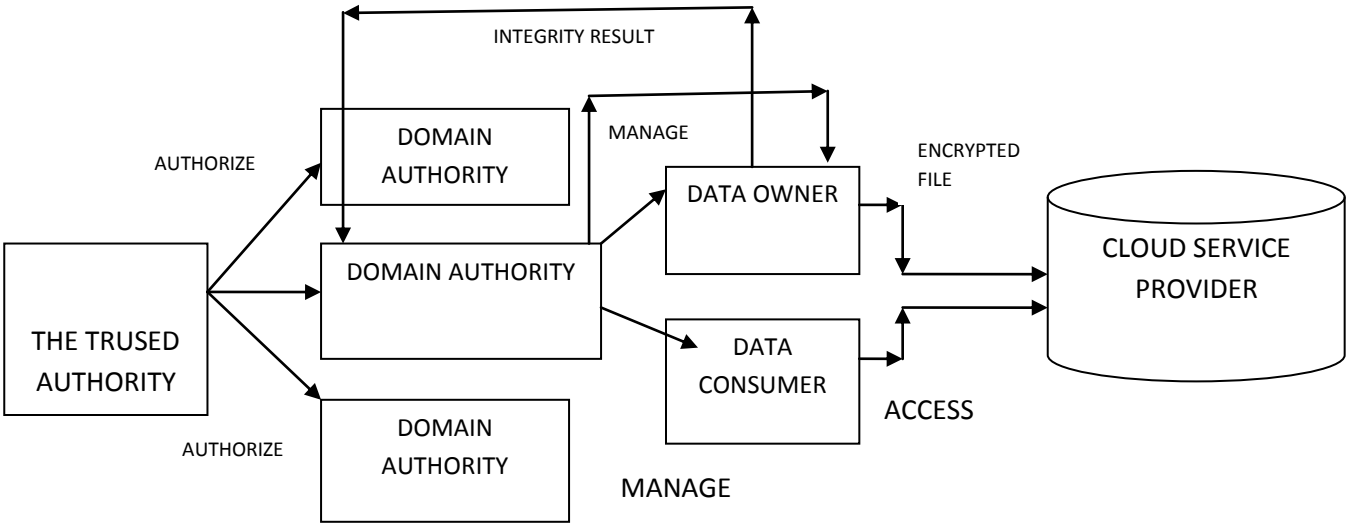
Data Consumers:
Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities.

Data Owners:
Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies.

Cloud Server:
Then, the owner sends the encrypted data to the cloud server together with the cipher-texts. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the cipher text; the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.

User Revocation Based ABE ALGORITHM:
The concept of **attribute based encryption** is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent about attributes. In a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.
Step 1: Select File attribute1 – say File name
Step 2: Convert the file name to Binary Codes
Step 3: Select File attribute 2 – say file size
Step 4 : Convert the file size to Binary Codes
Step 5: Perform AND Operation of File Attribute 1 and 2
Step 6: Perform OR Operation of File Attribute 1 and 2
Step 7: Result of AND Operation Stored as Secret Key
Step 8: Result of OR Operation Stored as Public Key

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 09
May 2016



7.CONCLUSION

This paper proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information. More importantly, our system can tolerate up to N − 2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis which shows that Anony-Control both secure and efficient for cloud storage system. The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer. One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes who support efficient user revocation is one of our future works.

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.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" n 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 riage And Semantic.

[7] A. Shamir, "Identity-based cryptosystems and signature schemes,"in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[8] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advancesin Cryptology*. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13thCCS*, 2006, pp. 89–98.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE SP*, May 2007, pp. 321–334.

[11] M. Chase, "Multi-authority attribute based encryption," in *Theory of Cryptography*. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.

[12] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proc. 16th CCS*, 2009, pp. 121–130.

[13] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," *Inf. Sci.*, vol. 180, no. 13, pp. 2618–2632, 2010.

[14] V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," *Int. J. Comput. Math.*, vol. 89, no. 3, pp. 268–283, 2012.