ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

Manipulation of Unauthorized Authorities by Using Deniable ABE Scheme

N.Devika[1], Dr.I.Hemalatha[2], Atyam Naga V S D Sri Veena[3], P.lavanya[4], V.R.B.Rohini[5]

Asst. Professor, Dept. of Information Technology, SRKREC, Bhimavaram, India [1]

Assoc. Professor, Dept. of Information Technology, SRKREC, Bhimavaram, India [2]

Asst. Professor, Dept. of Information Technology, SRKREC, Bhimavaram, India [3]

Asst. Professor, Dept. of Information Technology, SRKREC, Bhimavaram, India [4]

Asst. Professor, Dept. of Information Technology, SRKREC, Bhimavaram, India [5]

ABSTRACT: There are many cloud storage encryption schemes for protecting data from unauthorized users. However, some security schemes are compromised by some unauthorized authorities, to avoid this problem deniable encryption scheme is used. By using this scheme fake data is sent to the unauthorized users, this may not be possible all the time if the unauthorized users are aware of the data present. So, to handle this problem in this paper new scheme is explained in which while giving the input data is divided into 2 parts normal data and most important data (passwords, account numbers etc) the data which is marked as most important data will be sent as fake when an unauthorized user accessed and the normal data is sent as it is. So that the unauthorized user is manipulated.

KEYWORDS: Cloud storage provider, Deniable ABE Schemes, Secret key, Audit-free cloud, fake user.

I. INTRODUCTION

Hiding platform and implementation details unlimited virtualized resources provided to the users as a service is a cloud computing. [2]Presently cloud service provided to the users offered high available storage and massively parallel computing of resources at relatively low costs. But the question is about the cloud users with different privileges store data on cloud is a most challenging issue in managing cloud data storage system. Most important problem for cloud environment is privileges.

[3]Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Another potential benefit is that information may be better protected in the cloud. Predominantly, while there are benefits, there are privacy and security concerns too. The current system is based on Deniable Attribute Based Encryption scheme where encryption and decryption methodology is used. [5]Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in cipher texts such that outside coercers are satisfied. The attribute based encryption uses an attribute for the key that is generated. We make use of this idea, such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data. In our approach, the key distributor generates a unique key for the file to the user who has access to the respected files. When a user tries to access the file which has not been permitted for that user, the cloud admin marks him as the attacker. Thus maintaining privacy and security at high standards.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

[4]In cloud, data owner can store their data and access their data anywhere at any time from the cloud. The main aim of this paper is to protect data from the outside hackers. Our proposed scheme is used not only for the protection which is also to convince the hackers by the fake files and who cannot find whether the accessed file is true or not. Some of the proposed schemes assume storage providers in cloud are safe and cannot be hacked; however, in practice, some coercers may intercept communications between the data owner and the storage provider and force, storage provider to release owner's secrets or confidential data by using some government power in cloud.

In such case, the storage providers are requested to reveal user secrets. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant. Once cloud storage providers are compromised, all encryption schemes lose their effectiveness in the previous schemes. But In our scheme, storage providers can fight against such coercers to maintain the user privacy. Therefore, user privacy is still protected.

II. LITERATURE SURVEY

[10]A unified scheme for resource protection in automated trust negotiation Ting Yu , Winslett, M

Automated trust negotiation is an approach to establishing trust between strangers through iterative disclosure of digital credentials. In automated trust negotiation, access control policies play a key role in protecting resources from unauthorized access. Unlike in traditional trust management systems, the access control policy for a resource is usually unknown to the party requesting access to the resource, when trust negotiation starts. The negotiating parties can rely on policy disclosures to learn each other's access control requirements. However a policy itself may also contain sensitive information. Disclosing policies' contents unconditionally may leak valuable business information or jeopardize individuals' privacy. This paper proposing UniPro, a unified scheme to model protection of resources, including policies, in trust negotiation. UniPro improves on previous work by modeling policies as first-class resources, protecting them in the same way as other resources, providing fine-grained control over policy disclosure, and clearly distinguishing between policy disclosure and policy satisfaction, which gives users more flexibility in expressing their authorization requirements. It also show that UniPro can be used with practical negotiation strategies without Jeopardizing autonomy in the choice of strategy, and present criteria under which negotiations using UniPro are guaranteed to succeed in establishing trust.

[5]Cipher text-Policy Attribute Base Decryption John Bethencourt, Amit Sahai, Brent Waters

In several distributed systems a user should only be able to access data if a user posses a certain 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. This paper presenting a system for realizing complex access control on encrypted data that call Ciphertext-Policy Attribute-Based Encryption. By using this techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, this methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in this system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, these methods are conceptually closer to traditional access control methods such as Role-Based Access Control. In addition, it provides an implementation of our system and give performance measurements.

[3]Fuzzy Identity Based Encryption Amit Sahai , Brent R. Waters

This introduce a new type of Identity Based Encryption scheme that it call Fuzzy Identity Based Encryption. A Fuzzy IBE scheme allows for a private key for an identity id to decrypt a ciphertext encrypted with another identity id if and only if the identities id and id # are close to each other as measured by some metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric measurements as identities. The error-tolerance of a Fuzzy IBE scheme is

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

precisely what allows for the use of biometric identities, which inherently contain some amount of noise during each measurement.

[4]Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

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. We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption. In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption.

[14]Deniable Encryption with Negligible Detection Probability

An Interactive Construction Deniable encryption, introduced in 1997 by Canetti, Dwork, Naor, and Ostrovsky, guarantees that the sender or the receiver of a secret message is able to “fake” the message encrypted in a specific cipher text in the presence of a coercing adversary, without the adversary detecting that he was not given the real message. To date, constructions are only known either for weakened variants with separate “honest” and “dishonest” encryption algorithms or for single-algorithm schemes with non-negligible detection probability. We propose the first sender-deniable public key encryption system with a single encryption algorithm and negligible detection probability. We describe a generic interactive construction based on a public key bit encryption scheme that has certain properties, and we give two examples of encryption schemes with these properties, one based on the quadratic residuosity assumption and the other on trapdoor permutations.

[11]Deniable Encryption

Consider a situation in which the transmission of encrypted messages is intercepted by an adversary who can later ask the sender to reveal the random choice used in generating the cipher text, thereby exposing the clear text. An encryption scheme is deniable if the sender can generate ‘fake random choices’ that will make the cipher text ‘look like’ an encryption of a different clear text, thus keeping the real clear text private. Analogous requirements can be formulated with respect to attacking the receiver and with respect to attacking both parties. Deniable encryption has several applications, It can be incorporated in current protocols for incoercible voting, in a way that eliminates the need for physically secure communication channels. It also underlies recent protocols for general incoercible multiparty computation. Deniable encryption also provides a simplified and elegant construction of an adaptively secure multiparty protocol. In this paper we introduce and define deniable encryption and propose constructions of such schemes. Our constructions, while demonstrating that deniability is obtainable in principle, achieve only a limited level of it. Whether they can be improved is an interesting open problem.

III. PROBLEM STATEMENT

The problem is to determine, public auditing for such shared data while preserving identity privacy remains to be an open challenge. Unique problem introduced during the process of public auditing for shared data in the cloud is how to preserve identity privacy from the Third Party Auditor.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

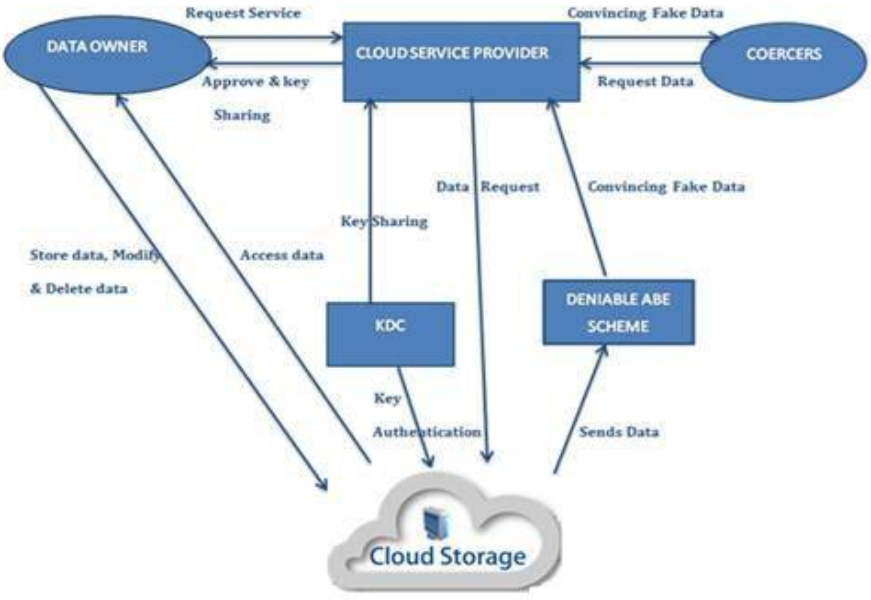
Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

IV.ALGORITHM

Setup (1) → (PP,MSK): This algorithm takes security parameter as input and returns public parameter as PP and system master key MSK.
KeyGen(MSK,S) → SK : Given set of attributes S and MSK. This algorithm outputs private key SK.
Enc(PP,M,A) →C : This encryption algorithm takes as input public parameter PP, message M and LSSS access structure A=(M,) over the universe of attributes, This algorithm encrypts M and outputs a cipher text C, which can be decrypted by those who possess an attribute set that satisfies access structure A. Note A is contained in C.
Verify(PP,C,M, PE, PD) → {T, F}: This algorithm is used to verify the correctness of PE and PD.
OpenEnc(PP,C,M) → PE: This algorithm is for the sender to release encryption proof PE for (M,C).
OpenDec(PP, SK,C,M) → PD: This algorithm is for the receiver to release decryption proof PD for(M,C).
Dec(PP, SK,C) → {M,⊥}: This decryption algorithm takes as input public parameter PP, private key SK with its attribute set S, and ciphertext C with its access structure A. If S satisfies A, then this algorithm returns M.

V. SYSTEM ARCHITECTURE



DATA OWNER

Firstly the data owner is registered with cloud service provider by submitting details like name, password and email. After getting registered the data owner uploads the data in the cloud by marking data as normal and important for security reasons data will be encrypted and the stored in cloud server.

CLOUD SERVER

Cloud server stores the most important data and normal data. The cloud server is responsible for data storage and files authorization and file search for an end user. The encrypted data file contents will be stored with their tags such as file

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

name, domain, Technology, Author, Publication, secret key, digital sign, date and time and owner name. Most important data is only encrypted in this scheme. The data owner is also responsible for adding data owner and to view the data owner files. The owner can conduct keyword search operations on behalf of the data users, the keyword search based on keywords (Author, Technology, Domain, publishers) will be sent to the Trust authority. If all are trustable then it will send to the corresponding user or he will be captured as attacker. The cloud server can also act as attacker to modify the data which will be auditing by the audit cloud. i.e, most import data will be modified and some fake data will be sent the unauthorized authority

KEY DISTRIBUTION CENTER

KDC is responsible for sharing of keys. When the data owner tries to register with cloud the KDC sends a secret key to the owner. The data owner encrypts and places the data in cloud KDC sends encrypted key to the trusted user when the user wants to access the data. The encrypted key will be decrypted using the key sent at the time of registration and with the decrypted key the data will be decrypted.

DATA CONSUMER

The data consumer can access the data with the encrypted key so if the user access the file by the wrong key then user will consider as malicious user and the user will be blocked

VI. EXPERIMENTAL RESULTS

Accessing the cloud server via randomized key protocol is highly secured. In the randomized key algorithm, the unique key generated by the key distributor provides security to the users. This method uses an audit free storage, which skips the third party auditing of the data and files that has been uploaded onto the cloud server. The key generated varies for each file and for each user. This proposed protocol is thus highly secured compared to the existing system.

VII. CONCLUSION

In this method we provide a cloud storage which is highly secured using randomised key protocol this makes coercers invalid. In our proposed scheme the master key is encrypted and distributed to the user so, that the fake user cannot hack.

REFERENCES

[1]N.Devika, Ch. Dileep Chakravarthy, " Public Auditing For Cloud Storage in Assessment Free Using Deniable ABE Scheme". IJIRCCE, VOL.4, Issue 9, September 2016, ISSN(ONLINE): 2320-9801.
[2]Po-Wen Chi, Chin-Laung Lei, "Audit-Free Cloud Storage via Deniable Attribute-based Encryption", IEEE Transactions on Cloud Computing, , no. 1, pp. 1, PrePrints , doi:10.1109/TCC.2015.2424882
[3]A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Eurocrypt, 2005, pp. 457–473.
[4]V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.
[5]J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.
[6]B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography, 2011, pp. 53–70.
[7]A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in Crypto, 2012, pp. 199– 217.
[8]S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public Key Cryptography, 2013, pp. 162–179.
[9]P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds." IEEE T. Cloud Computing, pp. 172–186, 2013.
[10]Wikipedia. (2014) Global surveillance disclosures (2013present). [Online]. Available: http://en.wikipedia.org/wiki/Global surveillance disclosures (2013-present)
[11]R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption," in Crypto, 1997, pp. 90–104.
[12]A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Eurocrypt, 2010, pp. 62–91