ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 5, NOVEMBER 2014, PP 271-276

PABKE: Provable Attribute-based Keyword explore over Outsourced Encrypted Data

G Pavan Kumar [1], Korathala Sreekanth Reddy [2], Chittem Raviteja [3], Shaik Mohammed Arif [4]
Department of CSE, G.Pullaiah College of Engineering and Technology. Kurnool
JNTU Anatapur, Andhra Pradesh, India

Abstract:-Cloud Computing has changed the phenomena of IT industry completely. It allows access to highly scalable, inexpensive, on demand computing resources that can execute the code and store data that are provided. But adoption and approach to cloud computing applies only if the security is ensured. Cloud computing is lacking in security, confidentiality and visibility. Secure the cloud means to secure the storage. Security is achieved by the encryption. There are various encryption standards to ensure the cloud security. Attribute-based encryption (ABE) is public key encryption technique that allows users to encrypt and decrypt messages based on user attributes. In a typical implementation, the size of the cipher text is proportional to the number of attributes associated with it and the decryption time is proportional to the number of attributes used during decryption. To reduce the decryption time in cloud outsourced decryption technique is used. By providing a transformation key to the cloud ABE cipher text is converted into simple cipher text and it only incurs a small computational overhead for the user to recover the plaintext from the transformed ciphertext.. To ensure that transformation performed by cloud server is correct and the data is not modified by the untrusted servers proposed system is introduced. This provides secured and Verifiable Outsourced decryption.

Keywords: Attribute Based Encryption, Ciphertext Policy Attribute Based Encryption, Cloud Computing, Key Policy Attribute Based Encryption.

1. INTRODUCTIONS

In Recent years cloud computing technology prototypes have exceedingly become a new way to provide shared services and data over the internet. Especially this prototype encourages an effective way of data sharing among the users of cloud, since the users are able to export the data to a public cloud storage which can provide access to data as a service .Considering this new model questions are raised as far the security if the services are concerned. To reduce costs and improve productivity and efficiency organizations across the globe look at technology as an essential part. The new advancements in cloud computing technology help organizations in reducing the computing costs while boosting work productivity. With ever increasing interest in cloud services and technology and the rise of Software As a Service(Saas) based applications the requirements for cloud based technologies is accelerating Apart from this with growing influence of web 2.0 technologies, non-enterprise users are also massively using cloud computing technologies. In the upcoming age cloud services will become the Cornerstone of the modern commercial world. In spite of cloud technology's tremendous capacity, there are still many technical hurdles that continue to hamper the wide spread adaption the technology. [1] Recent Privacy threats experienced by users of services offered by Apple, Google, Amazon [1] are clear indications that cloud is internally insecure from the users perspective. Because users don't have access to cloud service providers internal operations preserving privacy of user in cloud computing environment is a Challenge for researchers.Yanbin Lu and Gene Tsudik [2] list following challenges in preserving privacy in cloud.

Challenge 1: How to protect user private data from abuse by the cloud server?

Challenge 2: While using SaaS applications on cloud computing technology

Organizations outsource their data to cloud server? How to protect such outsourced data?

Challenge 3: How to query the cloud server without exposing query details?

Challenge 4: How to query contents from untrusted entities?

Challenge 5: How to design and implement content level fine-grained access control for users?

Up till now lot of work has been done to conserve the privacy in cloud server databases. Siani Pearson, Yun Shen and Miranda Mowbray [3] proposed a privacy manager for cloud computing. Jianwang [4] proposed anonymity based method for preserving cloud privacy. Miao Zhou [5] proposed a method for improved key management for maintaining privacy. Qin Liu [6] proposed bilinear graph based privacy preserving keyword searching method for accessing files. HaiboHu [7] proposed comprehensive privacy preserving scheme for indexed data. Marten van Dijk and Ari Juels [8] argued that alone cryptography is insufficient to maintain the privacy in cloud computing. Yanbin Lu and Gene Tsudik [9]

Proposed most comprehensive scheme that preserves the privacy and gives substantial improvements in encrypted database search, attribute-based encryption and predicate encryption. ShuchengYu [10] proposed Fine-grained Data Access Control in Cloud Computing using attribute based encryption. Although many schemes have been suggested to protect the privacy in cloud computing, most of them have not been able to resolve all the above listed challenges.

2. RELATED WORK:

Proxy Re-Encryption: In this process perform how to delegate (in a true offline sense) the ability to transform an ABE cipher text on message m into an El Gama style cipher text on the same m, without learning Anything about m. It is similar to the concept of proxy re-eccryption.where an untrusted proxy is given a re-encryption key that allows it to transform an encryption under Alice's key of m into an encryption under Bob's key of the same m, without allowing the proxy to learn anything about m

Pairing Delegation: It enables a client to outsource the computation of parings to another entity. However, the schemes proposed in [14], [15] still require the client to compute multiple exponentiations in the target group for every pairing it outsources. Most importantly, when using paring delegation i n the decryption o f ABE cipher texts.

3. PRESENTED SYSTEM:

Existing solutions for keyword search over encrypted data can be classified into two categories: searchable encryption in the symmetric-key setting and searchable encryption in the public-key setting In cipher text policy attribute-based Encryption (CP-ABE), every secret key is associated with a set of attributes, and every cipher text is associated with an access structure on attributes. Decryption is enabled if and only if the user's attribute set satisfies the cipher text access structure. Using (CP-ABE) any encryptor to specify access control in terms of any access formula over the attributes in the system. In the existing system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula. The Concept of verifiable is not described in detail in the existing system. The introduced cipher text policy attribute based encryption is the new way for the encryption. The encryption is fully based on the user attributes.

ABE is a new vision of public key based one-to-many encryption that enables access control over encrypted data using access policies and ascribed attributes associated with private keys and cipher texts. There are Two kinds of ABE schemes:

1. Cipher text-policy ABE (CP-ABE).
2. Key-policy ABE (KP-ABE)

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 5, NOVEMBER 2014, PP 271-276

In a CP-ABE scheme [8], [9], [5], [6] each cipher text is associated with an access policy according to the attributes. The user's private key is associated with a set of attributes. This user is able to decrypt a cipher text. If the set of attributes associated with the user's private key satisfies the access policy.

In a KP-ABE Scheme [2]–[7] the parts of a quality set and a right to gain entrance strategy are swapped from what we depicted for CP-ABE: ascribes sets are utilized to clarify the figure writings and access polices over these qualities are connected with user's private keys.

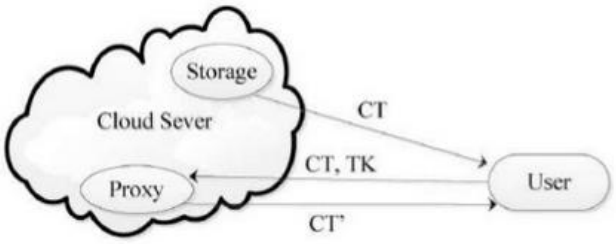


Fig 1: ABE system with outsourced decryption.

In the fig[1] it refers a user provides an untrusted server, say as a proxy operated by a cloud service provider, with a transformation key TK that allows to translate any ABE cipher text CT satisfied by that user's attributes or access policy into a simple cipher text CT'.Most of the existing systems are proposed the attribute based encryption with various limitations and low performance to produce the cipher text. Whenever we use the attribute based encryption the length of the cipher text is greater to the proportion of the plain text size.

Demerits:

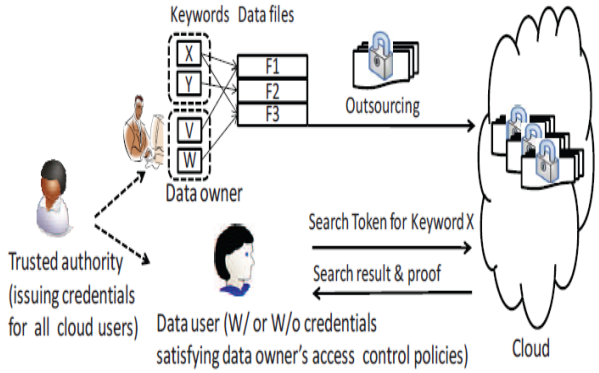
- No error recovery algorithms are implemented in existing system.
- No methods to verify the transformation.
- The untrusted server can perform the transformation in the sensitive data wrong transformations may lead to problems.
- Decryption time is high.

4. PROPOSED SYSTEM:

The Problem in the Existing system is the user cannot trust the transformation performed by an untrusted server. To overcome that problem the proposed system contains a checksum to verify the correctness of the transformation. The system proposed method is a verifiable approach. The goal of the proposed system is to reduce the decryption time on the user side. According to that the proposed system allows to perform a transformation over the cipher text. The transformation process reduces the size of the cipher text. Even the transformation is performed the file reminds as in the cipher text form and not in a fully decrypted form. Then the user can decrypt the file with his secret key. The problem of the verification overcame here. We provide a checksum value for the each file. Whenever the user receives a file also receives the corresponding checksum. The user then produces the checksum for the received file and checks whether the both are same or not. If both are same then the transformation is correct otherwise wrong. Merits:

- The proposed system let the user to verify the cloud server transformation.
- The proposed system is verifiable but not with compromised with security.
- It is a new approach for outsourcing encryption that let the user to verify.
- It guarantees that the adversary cannot be able to learn anything about the encrypted cipher text.

5. SYSTEM ARCHITECTURE:-



ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 5, NOVEMBER 2014, PP 271-276

6. SYSTEM DESCRIPTION

6.1. Cloud Computing

Cloud computing is the provision of dynamically scalable and often virtualized resources as a services over the internet Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud computing represents a major change in how we store information and run applications. Instead of hosting apps and data on an individual desktop computer, everything is hosted in the "cloud"—an assemblage of computers and servers accessed via the Internet.

Cloud computing exhibits the following key characteristics:

1. **Agility** improves with users' ability to re-provision technological infrastructure resources.

2. **Cost is** claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation. The e-FISCAL project's state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house

3. **Virtualization** technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.

4. **Multi tenancy** enables sharing of resources and costs across a large pool of users thus allowing for:

5. **Centralization** of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

6. **Utilization and efficiency** improvements for systems that are often only 10–20% utilized.

7. **Reliability** is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

8. **Performance** is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

9. **Security** could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

10. **Maintenance** of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

6.2. Trusted Authority

A trusted authority, which issues credentials to the data owners/users. The data owners are naturally

trusted. Both authorized and unauthorized data users are semi-trusted, meaning that they may try to infer some sensitive information of interest. The cloud is not trusted as it may manipulate the search operations, which already implies that the cloud may manipulate the outsourced encrypted data.

6.3. Attribute-based keyword search

We use ABE to construct a new primitive called attribute-based keyword search, by which keywords are encrypted according to an access control policy and data users with proper cryptographic credentials can generate tokens that can be used to search over the outsourced encrypted data. This effectively prevents a data owner from the keywords a data user is searching for, while requiring no interactions between the data users and the data owners/trusted authorities.

6.4. Encryption-Decryption

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor decryption is the reverse process to Encryption. Frequently, the same Cipher is used for both Encryption and Decryption. While Encryption creates a Ciphertext from a Plaintext, Decryption creates a Plaintext from a Ciphertext.

7. CONCLUSION

We have introduced a novel cryptographic primitive called verifiable attribute-based keyword search for secure cloud computing over outsourced encrypted data. This primitive allows a data owner to control the search of its outsourced encrypted data according to an access control policy, while the authorized data users can outsource the search operations to the cloud and force the cloud to faithfully execute the search (as a cheating cloud can be held accountable). Performance evaluation shows that the new primitive is practical. Our study focused on static data. As such, one interesting open problem for future research is to accommodate dynamic data.

REFERENCES:

1. Kui Ren, Cong Wang, and Qian Wang, "Security Challenges for the Public Cloud", Internet Computing, IEEE, Vol. 16, Issue 1,Jan.-Feb. 2012.

2. Y. Lu and G. Tsudik, "Privacy-Preserving Cloud Database Querying", Journal of Internet Services and Information Security (JISIS), Vol. 1, No. 4, November 2011.

3. Siani Pearson, Yun Shen, Miranda Mowbray, "A Privacy Manager for Cloud Computing", First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings

4. Jian Wang, Yan Zhao, Shuo Jiang, Jiajin Le, "Providing privacy preserving in cloud computing", Test and Measurement, vol. 2, ICTM '09, International Conference, 2009.

5. Miao Zhou , Yi Mu , Willy Susilo , Jun Yan , Liju Dong, "Privacy enhanced data outsourcing in the cloud, Journal of Network and Computer Applications", vol. 35, issue 4, pp. 1367–1373, 2012.

6. Qin Liu, Guojun Wang, Jie Wu, "Secure and privacy preserving keyword searching for cloud storage services", Journal of Network and Computer Applications, vol. 35, pp. 927–933, 2012.

7. Haibo Hu, Jianliang Xu , Chushi Ren , Byron Choi, "Processing private queries over untrusted data cloud through privacy homomorphism" , Data Engineering (ICDE), 2011.

8. Marten Van Dijk, Ari Juels, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing", IACR Cryptology eprint Archive, 2010.

9. Dr. Alexander Benlian, Prof. Dr. Thomas Hess, Prof. Dr. Peter Buxmann, "Drivers of SaaS-Adoption – An Empirical Study of Different Application Type", Business & Information Systems Engineering, Vol. 1, Issue 5, pp 357-369, October 2009.

10. Shucheng Yu Cong Wang, Kui Ren , Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", INFOCOM, 2010 Proceedings IEEE.

11. Vipul Goyal,Omkant Pandey, Amit Sahai, Brent Waters , "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", Proceeding CCS '06 Proceedings of the 13th ACM conference on Computer and communications security Pages 89 - 98 ,ACM New York, NY

12. John Bethencourt, Amit Sahai, Brent Waters, "Ciphertext-Policy Attribute-Based Encryption, Security and Privacy", 2007.

13. M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryptionof ABE ciphertexts," in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.

14. Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng, "Attribute-Based Encryption With Verifiable Outsourced Decryption", IEEE Transaction on Information Forensics and Security, vol. 8, no. 8, August 2013.