ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

A Survey on Secure Data Self-Destructing Scheme in Cloud Computing

Rohit Bamane[1], Nikhil Tarukhakar[2], Prashant Pandit[2], Nikesh Mhaske[2], Swaminath Shitole[2]

Assistant Professor, Dept. of CS, Pad.Dr.D.Y.Patil Institute Of Engineering And Technology, Pimpri, Savitribai Phule Pune University, Pune, India

Students, Dept. of CS, Pad.Dr.D.Y.Patil Institute Of Engineering And Technology,Pimpri, Savitribai Phule Pune University, Pune, India

ABSTRACT:-With the rapid development of versatile cloud services, it becomes increasingly susceptible to use cloud services to share data in a friend circle in the cloud computing environment. Since it is not feasible to implement full lifecycle privacy security, access control becomes a challenging task, especially when it share sensitive data on cloud servers. In order to tackle this problem, So a key-policy attribute-based encryption with time-specified attributes (KP-TSABE), a novel secure data self-destructing scheme in cloud computing. In the KP-TSABE scheme, every cipher text is labelled with a time interval while private key is associated with a time instant. The cipher text can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the cipher text satisfy the key's access structure. The KP-TSABE is able to solve some important security problems by supporting user defined authorization period and by providing fine-grained access control during the period. The sensitive data will be securely self-destructed after a user-specified expiration time. The KP-TSABE scheme is proved to be secure under the decision l-bilinear Diffie-Hellman inversion (l-Expanded BDHI) assumption. Comprehensive comparisons of the security properties indicate that the KP-TSABE scheme satisfies the security requirements and is superior to other existing schemes.

KEYWORDS: Sensitive data, secure self-destructing, fine-grained access control, privacy-preserving, cloud computing

I. INTRODUCTION

Distributed computing is considered as the following stride in the advancement of on-interest information innovation which joins an arrangement of existing and new systems from exploration zones, for example, administration situated architectures (SOA) and virtualization. With the quick improvement of flexible distributed computing innovation and administrations, it is normal for clients to influence distributed storage administrations to impart information to others in a companion circle, e.g., Dropbox, Google Drive and Ali Cloud The mutual information in cloud servers, then again, as a rule contains clients' touchy data (e.g., individual profile, financial information, wellbeing records, and so on.) and should be very much ensured As the responsibility for information is isolated from the organization of them.

The cloud servers may relocate clients' information to other cloud servers in outsourcing or offer them in cloud seeking. Accordingly, it turns into a major test to ensure the protection of that mutual information in cloud, particularly in cross-cloud and enormous information environment. With a specific end goal to meet this test, it is important to outline a thorough answer for bolster client defined approval period and to give fine-grained access control amid this period. The common information ought to act naturally wrecked after the client defined expiration time.

II. RELATED WORK

1. ORUTA: PRIVACY-PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD.[1] From this paper we Referred-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information-identity privacy-to public verifiers. So a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, it exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity.

2. PRIAM: PRIVACY PRESERVING IDENTITY AND ACCESS MANAGEMENT SCHEME IN CLOUD.[2]
From this paper we Referred-

Each cloud service has numerous owners and tenants, so it is necessary to construct a privacy preserving identity management and access control mechanism for cloud computing. On one hand, cloud service providers (CSP) depend on tenant's identity information to enforce appropriate access control so that cloud resources are only accessed by the authorized tenants who are willing to pay. On the other hand, tenants wish to protect their personalized service access patterns, identity privacy information and accessing newfangled cloud services by on-demand ways within the scope of their permissions. There are many identity authentication and access control schemes to address these challenges to some degree, however, there are still some limitations. A new comprehensive approach, called Privacy pReserving Identity and Access Management scheme, referred to as PRIAM, which is able to satisfy all the desirable security requirements in cloud computing. The main contributions of the PRIAM scheme are threefold. First, it leverages blind signature and hash chain to protect tenant's identity privacy and implement secure mutual authentication. Second, it employs the service-level agreements to provide flexible and on-demand access control for both tenants and cloud services. Third, it makes use of the BAN logic to formally verify the correctness of the protocols. As a result, PRIAM scheme is suitable to cloud computing thanks to its simplicity, correctness, low overhead, and efficiency.

3. CLOUD MIGRATION RESEARCH: A SYSTEMATIC REVIEW.[3]
From this paper we Referred-

Background--By leveraging cloud services, organizations can deploy their software systems over a pool of resources. However, organizations heavily depend on their business-critical systems, which have been developed over long periods. These legacy applications are usually deployed on-premise. In recent years, research in cloud migration has been carried out. However, there is no secondary study to consolidate this research. Objective--This paper aims to identify, taxonomically classify, and systematically compare existing research on cloud migration. Method is conducted a systematic literature review (SLR) of 23 selected studies, published from 2010 to 2013. So it classified and compared the selected studies based on a characterization framework that also introduce. Results--The research synthesis results in a knowledge base of current solutions for legacy-to-cloud migration. This review also identifies research gaps and directions for future research. Conclusion--This review reveals that cloud migration research is still in early stages of maturity, but is advancing. It identifies the needs for a migration framework to help improving the maturity level and consequently trust into cloud migration. This review shows a lack of tool support to automate migration tasks. This study also identifies needs for architectural adaptation and self-adaptive cloud-enabled systems.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

4. TOWARD EFFICIENT AND PRIVACY-PRESERVING COMPUTING IN BIG DATA ERA[4]
From this paper we Referred-

Big data, because it can mine new knowledge for economic growth and technical innovation, has recently received considerable attention, and many research efforts have been directed to big data processing due to its high volume, velocity, and variety (referred to as "3V") challenges. However, in addition to the 3V challenges, the flourishing of big data also hinges on fully understanding and managing newly arising security and privacy challenges. If data are not authentic, new mined knowledge will be unconvincing; while if privacy is not well addressed, people may be reluctant to share their data. Because security has been investigated as a new dimension, "veracity," in big data, in this article, aim to exploit new challenges of big data in terms of privacy, and devote our attention toward efficient and privacy-preserving computing in the big data era. Specifically, So it first formalize the general architecture of big data analytics, identify the corresponding privacy requirements, and introduce an efficient and privacy-preserving cosine similarity computing protocol as an example in response to data mining's efficiency and privacy requirements in the big data era.

5. SCALABLE, SERVER-PASSIVE, USERANONYMOUSTIMED RELEASE CRYPTOGRAPHY.[5]
From this paper we Referred-

It consider the problem of sending messages into the future, commonly known as timed release cryptography. Existing schemes for this task either solve the relative time problem with uncontrollable, coarse-grained release time (time-lock puzzle approach) or do not provide anonymity to senders and/or receivers and are not scalable (server-based approach). Using a bilinear pairing on any Gap Diffie-Hellman group, solve this problem by giving scalable, server-passive and user-anonymous timed release public-key encryption schemes allowing precise absolute release time specifications. Unlike the existing server-based schemes, the trusted time server in our scheme is completely passive - no interaction between it and the sender or receiver is needed; it is even not aware of the existence of a user, thus assuring the privacy of a message and the anonymity of both its sender and receiver. Besides, our scheme also has a number of desirable properties including a single form of update for all users, self-authenticated time-bound key updates, and key insulation, making it a scalable and appealing solution. It could also be easily generalized to a more general policy lock mechanism

III. PROPOSED METHODOLOGY

Data owner can provide data orfiles that contain some sensitive information, whichare used for sharing with his/her friends (data users). All these shared data are outsourced to the cloudservers to store. Authority is an indispensable entity which is responsible for generating, distributing and managing all the private keys, and is trusted by all the other entities involved in the system. Time Server is a time reference server without any interaction with other entities involved in the system. It is responsible for a precise release time specification. Data users are some peoples who passed the identity authentication and access to the data outsourced by the data owner. Notice that, the shared data can only be accessed by the authorized users during its authorization period. Cloud Servers contains almost unlimited storage space which is able to store and manage all the data or files in the system. Other entities with limited storage space can store their data to the cloud servers. Potential Adversary is a polynomial time adversary and described in the security model of the KP-TSABE scheme

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

IV. ARCHITECTURE

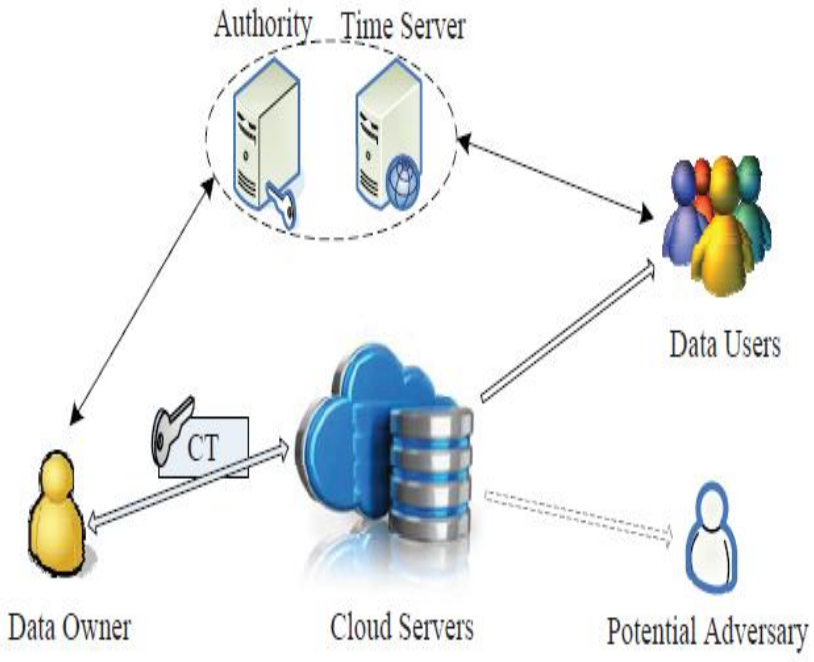

FIG NO 1. SYSTEM MODEL OF THE KP-TSABE SCHEME

V. CONCLUSION

Data privacy is essential in the Cloud environment. A new approach is introduced for protecting the data privacy from attackers which may obtain, from legal or other means, a user's stored data and private decryption keys. A novel aspect is the leveraging of the essential properties of active storage framework based on T10OSD standard. Personal data stored in the cloud may contain account numbers, secret codes and other necessary details that could be used and misused. SeDas uses the self-destruct operation without any action on the user's part. Measurement and experimental security analysis sheds insight into the practicability of this approach. Plan to release the current SeDas system will help to provide researchers with further valuable experience to inform future object-based storage system designs for Cloud services.

REFERENCES

1. B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," Cloud Computing, IEEE Transactions on, vol. 2, no. 1, pp. 43–56, 2014.
2. J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, "Priam: Privacy preserving identity and access management scheme in cloud," KSII Transactions on Internet and Information Systems (TIIS), vol. 8, no. 1, pp. 282–304, 2014.
3. P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud migration research:A systematic review," Cloud Computing, IEEE Transactions on,vol. 1, no. 2, pp. 142–157, 2013.
4. R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient and privacy-preserving computing in big data era," Network, IEEE, vol. 28, no. 4, pp. 46–50, 2014.
5. A. F. Chan and I. F. Blake, "Scalable, server-passive, user anonymous timed release cryptography," in Proceedings of the International Conference on Distributed Computing Systems. IEEE, 2005, pp. 504–513.