Review on Secure Sharing and Self Destructing Data on Cloud Computing

Arkile Rupali.A
Student
Department of Computer Engineering
S.B.Patil College of Engineering, Vangali, Indapur

Burkule Samruddhi.S
Student
Department of Computer Engineering
S.B.Patil College of Engineering, Vangali, Indapur

Lakade Sharmila. D
Student
Department of Computer Engineering
S.B.Patil College of Engineering, Vangali, Indapur

Nalawade Vinay. S
Assistant Professor
Department of Computer Engineering
S.B.Patil College of Engineering, Vangali, Indapur

Abstract

With the quick advancement of flexible cloud administrations, it turns out to be progressively helpless to utilize cloud administrations to share information in a companion hover in the distributed computing condition. Since it is not practical to actualize full lifecycle protection security, get to control turns into a testing errand, particularly when we share delicate information on cloud servers. Keeping in mind the end goal to handle this issue, we propose a key-approach trait based encryption with time-indicated characteristics (KP-TSABE), a novel secure information self-destructing plan in distributed computing. In the KP-TSABE plot, each figure content is marked with a period interim while private key is related with a period moment. The delicate information will be safely self-destructed after a client indicated termination time. Far reaching correlations of the security properties demonstrate that the KP-TSABE conspire proposed by us fulfills the security prerequisites and is better than other existing plans.

Keywords: Sensitive Data, Secure Self-Destructing, Privacy Preserving, Cloud Computing

I. INTRODUCTION

Cloud computing is a virtual concept. Cloud computing means storing and accessing data. The shared data in cloud servers, however, usually contains users sensitive information like Personally identifiable information or PII (e.g. Social Security numbers, phone numbers, home addresses, etc.),Protected health information or PHI (e.g. patient diagnoses, medical treatments, etc.)Payment data (e.g. credit card numbers, debit card numbers, bank accounts, etc.) ,Confidential data (e.g. financial records, business plans, top secret documents, source code, trading algorithms, etc.)In many circumstances, when a user encrypts delicate data. The main aspects are to provide feasibility, scalability and fine grained access control. To enable more general access control, proposed a key-policy attribute-based encryption (KP-ABE) scheme – a variant of ABE. The idea of a KP-ABE scheme is as follows: the cipher text is associated with a set of attributes and user secret key. A user is able to decrypt a cipher text if and only if the cipher text attributes pass the access structure embedded in her secret key. KP-ABE is suitable for applications such as IT Company sharing data over server, in which user access privileges are defined over content attributes and could be based on their designation, project they work on and department

II. LITERATURE SURVEY

A. "Vanish: Increasing Data Privacy with Self-Destructing Data"

Roxana Geambasu Tadayoshi Kohno Amit A. Levy Henry M. Levy [1] describes Personal data to be cached, copied, and archived by third parties, often without our knowledge. The disclosure of private data has become commonplace due to carelessness, theft, or legal actions. This exiting system presents Vanish, a system that meets this challenge through a novel integration of cryptographic techniques with global-scale, P2P; distributed hash tables (DHTs).The experience also reveals limitations of existing DHTs for Vanish-like applications. In Vuze, for example, the fixed data timeout and large replication factor present challenges for a self-destructing data system. For a future research is to redesign existing DHTs with our specific privacy applications in mind. Our plan to release the current Vanish system will help to provide us with further valuable experience to inform future DHT designs for privacy applications.

B. "Time Based Self-Destruction System for Secure Data Sharing in Cloud"

Harikrishnan G.R., Sreeja V., Pavithra T.P., Sithara A.P. [2]they describes the shared data in a dynamic environment remains in cloud for indefinite period of time and the sensitive information stored may bemisused by a miscreant or even by service providers.

In exiting system, a self-destructing module can be used to automatically clear the data and their copies after a user-specified time.By using AES-256 and triple DES algorithm such a system can be developed. In this paper, they proposed a secure self-destruction system in cloud computing. Data privacy has become increasingly important in the cloud environment. Thus for ensuring more security multiple encryption techniques were used. They also included a multi cloud feature for the recovery of the destructed file if it is further needed. Hence in this self-destruction system all the file are removed automatically as the time expires. They strongly believe that the system will reduce complexity in managing old data files and thereby increasing possibilities in reducing security and privacy issues.

C. *"SEDAS: A Self Destruction for Protecting Data Privacy in Cloud Storage as a Service Model"*

Lalitha K1, Sasi Devi J2 [3] describes in this paper personal data and other important information that could be used and misused by a miscreant, a competitor or a court of law. These data are cached, copied and archived by Cloud Service Providers (CSPs), often without user authorization and control. For this problem to propose a Self Destruction method ,this method is protecting the user data privacy by using Shamir Secret sharing algorithm, which can generate a pair of secret keys. During the download process the Shamir algorithm check the validity of this secret keys. If the secret keys are expired, The Shamir algorithm generate new pair of keys to the user through this only the SEDAS system meet all the privacy preserving goals. For future work of the SEDA system, they can increase the key length to provide user data privacy in cloud.

D. *"Secure File Transmission using Byte Rotation Algorithm in Netwok Security"*

Punam V. Maitri, Rekha V. Sarawade, Sarika T. Deokate, Mayuri P. Patil [4] describe in this paper Secure file transmission from one android user to another android user is important issue in network security. In this exiting system Byte rotation algorithm (BRA) and AES algorithm solve the problem of secure file transmission using encryption and decryption. By using BRA algorithm they achieved different important parameters like reduce the speed of encryption and decryption process and reduce complexity of algorithm. In this proposed system user can set time and frequency for secure file. When these conditions are satisfied File and key used for encryption will be deleted. They have implemented android application for provide security to different files like text, image, audio and video by using Byte rotation algorithm. The performance of BRA algorithm is 20 to 30% better for encryption and decryption as compared to AES algorithm. There for BRA algorithm gives very good performance for encryption and decryption of file .For future work they can increase performance of BRA algorithm.

E. *"MSC: Mobile Secure Communication Using SMS in Network Security: A Survey"*

Punam V. Maitri, Rekha V. Sarawade, Mayuri P. Patil,Sarika T. Deokate [5] decribes in this paper Information as well as SMS security is important and challenging part for mobile communication. Some ethical hackers or attackers access the illegally sensitive data or messages .In this exiting system the survey of SMS encryption as well as decryption techniques, algorithms, models use in communication network and security. Many users' uses the various algorithm and techniques for provide security to data and SMS in communication networks. Some users use encryption as well as decryption algorithms. The algorithms like AES, DES, Triple DES used by many authors for encrypt or decrypt SMS for communication. The concept of Server key secure and Sender key secure messaging for SMS security. In this paper they have do the survey of previous and new encryption as well as decryption android application and algorithms. Finally they here prove that the AES algorithm is secure, fast and strong encryption algorithm for mobile communication. In future work they have doing survey of the more encryption and decryption algorithms. And develop stronger, secure, and easy new algorithm for encryption and decryption for Android mobile communication.

F. *"Time Controlled Cloud Environment with Self destructing Data system (SeDas) for Data Confidentiality"*

S. Savitha1, Dr. D. Thilagavathy[6] describes in this paper Information are cached, copied, and archived by Cloud Service Providers (CSPs), typically for users' authorization and management. There are high chances for the data to fall into wrong side.SeDas system meets this challenge by a new combination of cryptographic techniques and active storage framework based on T10 OSD standard. In this proposed system security procedures and functionalities make sure that SeDas meets all privacy-preserving policies. SeDas is easy for practical use. For future work, the users are provided more advanced features for managing the files on the cloud server even after destruction. One time live factor expires the data with all the copies are destroyed. Sometimes the users are forced to enter into situations where the files might be in need for their personal verification. In order to make this happen the file has to be recovered back. In which it is difficult to find the data back, with the help of some strong security procedures this could be hopefully made more easy and enhanced by making cloud services ahead in the near future.

G. *"Cipher text-Policy Attribute-Based Encryption"*

John Bethencourt, AmitSahai, Brent Waters [7]describe in this paper,several distributed systems a user should only be able to access data if a user possesses a certain set of attributes. They present a system for realizing complex access control on encrypted data that we call Cipher text-Policy Attribute-Based Encryption.In this paper they present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. In the future, it would be interesting to consider attribute-based encryption systems with different types of impressibility. While, Key-Policy ABE and Cipher text-Policy

ABE capture two interesting and complimentary types of systems there certainly exist other types of systems. The primary challenge in this line of work is to find new systems with elegant forms of expression that produce more than an arbitrary combination of techniques.

II. "Cipher text-Policy Weighted Attribute Based Encryption for Fine-Grained Access Control"

Jianfeng Ma, JinboXiong, Qi Li, Jun Ma [8] describe in this paper the cipher text-policy attribute based encryption scheme, the private key hold by user is associated with a set of attributes while the data is encrypted with an access Structure defined by the data provider. They used a scheme called cipher text-policy weighted attribute based encryption (CP-WABE) while the attributes have different Weights according to their importance. This work motivates a few interesting problems in this paper, how can we construct more efficient CP-ABE schemes with weighted attributes and how can we revocation attributes in different weights more efficiently. Therefore, future work is how to design a CP-WABE scheme to solve these problems.

III. CONCLUSION

The concept of cloud computing provides a great opportunity to users to utilize their services on-demand basis. The requirement of mobility in cloud computing gave birth to Mobile cloud computing. MCC provides more possibilities for access services in convenient manner. It is expected that after some years a number of mobile users will going to use cloud computing on their mobile devices. There are many issues in mobile cloud computing due to limitations of mobile devices. Security is the main concern in mobile cloud computing. In Mobile Cloud Computing data of owner is stored on the cloud, which is not secured. This paper has provided the description about the basics of Mobile Cloud Computing and issues associated with it. Mainly it discussed about security of data stored in cloud and importance of data security. This paper has explored a number of mechanisms for providing data security so that Mobile Cloud Computing can be widely accepted by a number of users in future. It also provied a mechanism to confidentiality, access control as well as integrity to mobile In future the work can be done on the proposed scheme for providing data confidentiality with data integrity so that Mobile Cloud Computing will be widely accepted

REFERENCES

[1] Roxana Geambasu Tadayoshi Kohno Amit A. Levy Henry M. Levy," "Vanish: Increasing Data Privacy with Self- Destructing Data" published in 2007.
[2] Harikrishnan G.R., Sreeja V., Pavithra T.P., Sithara A.P, "Time Based Self-Destruction System for Secure Data Sharing in Cloud"published in IJCAT - International Journal of Computing and Technology, Volume 3, Issue 2, February 2016.
[3] Lalitha K1, Sasi Devi J2, "SEDAS: A Self Destruction for Protecting Data Privacy in Cloud Storage As A Service Model" published in IJIRSET Volume 3, Special Issue 1, February 2014.
[4] Punam V. Maitri, Rekha V. Sarawade, Sarika T. Deokate, Mayuri P. Patil "Secure File Transmission using Byte Rotation Algorithm in Netwok Security"I published in international Conference for Convergence of Technology - 2014.
[5] Punam V. Maitri, Rekha V. Sarawade, Mayuri P. Patil,Sarika T. Deokate "MSC : Mobile Secure Communication Using SMS in Network Security : A Survey"published in International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 11, November - 2013
[6] S. Savitha1, Dr. D. Thilagavathy "Time Controlled Cloud Environment with Self destructing Data system (SeDas) for Data Confidentiality" published inIOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. Nov – Dec. 2014.
[7] John Bethencourt, AmitSahai, Brent Waters "Cipher text-Policy Attribute-Based Encryption"published in 2007.
[8] Jianfeng Ma, JinboXiong, Qi Li, Jun Ma "Cipher text-Policy Weighted Attribute Based Encryption for Fine-Grained Access Control"published in 2013 IEEE