ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

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

[I]Shivam Mattoo, [II]Anmol Mattoo, [III]Rohan Raygade, [IV]Yash Singi,
[V]Deepali B. Gothawal, [VI]Vishakha A. Metre
[I,II,III,IV,V,VI]Dept. of Computer Engineering, D Y Patil College of Engineering, Akurdi, Pune (MH), India

Abstract
Cloud computing may be defined as management and provision of resources, software, applications and information as services over the cloud (internet) on demand. 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. The tremendous amount of data outsourced every day by individuals or each enterprises. It is impossible to manage or to store this complex data at individual level, as the chances of crash the system is more. Then the cloud came into picture to store the data with better flexibility and cost saving. Considering the privacy of the data over the cloud to preserve the confidentiality or sensitivity, a novel secure data self-destructing scheme in cloud computing i.e A key-policy attribute-based encryption with time-specified attributes (KP-TSABE), is used. In the KP-TSABE scheme, every cipher text is labeled with a time interval while private key is associated with a time instant. The ciphertext 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 keys access structure. The KP-TSABE is able to solve important security problems such as Data loss and Data corruption by supporting user defined authorization period and by providing fine-grained access control during the period. The storing of a large amount of data including critical information on the cloud motivates highly skilled hackers thus creating a need for the security to be considered as one of the top issues while considering Cloud Computing. This paper explains the cloud computing along with its open secure architecture advantages in brief and emphasize on various security threats in cloud computing also the existing methods to control them.

Keywords
Sensitive Data, Secure Self-Destructing, Fine-Grained Access Control, Privacy-Preserving, Cloud Computing

I. Introduction

Cloud computing is the collection of virtualized and scal-able resources, capable of hosting application and providing required services to the users with the pay only for use strategy where the users pay only for the number of service units they consume [3]. A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way. Every individual is producing tremendous amount of data than ever before, and this rate is only going to increase day by day. Also more importantly the organizations have much higher rate of producing data which is in fact more sensitive too. Hence, organizations are often more concerned about the security of there data to store it on cloud storage, all of this leads to the increased authenticatinon demand. Considering the privacy of the data over the cloud, the searching techniques should be good enough to not to expose the data publicly while searching. As an approach to retaining control of data on cloud is to make use of the encryption of all cloud data. The problem is that encryption limits data. The encrypted data becomes problematic in searching and indexing. Data stored in clear-text can be efficiently searched by specifying a keyword. This is not feasible to do with traditional encryption schemes. Enhanced and more sophesticated cryptography may offer new tools to make the data searchably encrypted. Encryption schemes like searchable encryption also known as predicate encryption that allow operation and computation on the ci-phertext, allows the data owner to compute a capability from his secret key [5]. A capability encodes a search query, and the cloud can use this capability to decide which documents match the search query, without the requirement of any additional information. Other cryptographic techniques such as homo-morphic encryption and Private Information Retrieval (PIR) perform computations on encrypted data without decrypting it [7]. More generally, self-destructing data is broadly applicable in todays Web-centered world, where users sensitive data can persist in the cloud indefinitely

Apart from introduction in section I, the paper is organized as follows- Cloud Computing System is explained in section II, Transparent Cloud Protection System (TCPS) is explained in section III, Client Based Privacy Manager is described in section IV, Section V concludes the paper.

II. Cloud Computing System

The mutual information in cloud servers, not with standing, typically contains clients delicate data and needs to be very much secured. 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 information search over cloud. It is important to improve arrangement to client approval period and to give regrained access control amid this period. Attribute Based En-cryption (ABE) has significant focal points taking into account the convention open key encryption of balanced encryption on the grounds that it accomplishes one to numerous encryption [8]. A Cloud Computing System is Depicted in fig.1. below:

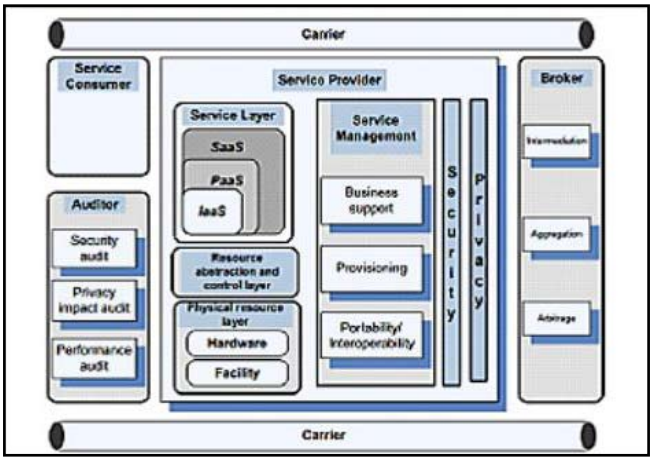

Fig. 1. Cloud Computing System [4]

The various modules of a Secure Cloud Computing System are as follows-

A. Service Consumers

It is an entity that maintains bussiness relationships and user services.

B. Service Provider

It is an entity responsible for making services available. Different Popular Cloud Service Providers are mentioned below:

1) Software as a Service(SaaS): The SaaS is not suitable for applications that require real-time response or those for which data is not allowed to be hosted externally. The most likely candidates for SaaS are applications for which:

- Many competitors use the same product, such as email.
- Periodically there is a significant peak in demand, such as billing and payroll.
- There is a need for Web or mobile access, such as mobile sales management software.
- There is only a short-term need, such as collaborative software for a project.

2) Platform as a Service(PaaS): Platform-as-a-Service (PaaS) gives the capability to deploy consumer-created or acquired applications using programming languages and tools supported by the provider. The user does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage. The user has control over the deployed applications and, possibly, over the application hosting environment configurations. Such services include session management, device integration, sandboxes, instrumentation and testing, contents management, knowledge management, and Universal Description, Discovery, and Integration (UDDI), a platform-independent Extensible Markup Language (XML)-based registry providing a mechanism to register and locate Web service applications. PaaS is not particulary useful when the application must be portable, when proprietary programming languages are used, or when the underlaying hardware and software must be customized to improve the performance of the application [4]. The major PaaS application areas are in software development where multiple developers and users collaborate and the deployment and testing services should be automated.

3) Infrastructure as a Service(IaaS): Infrastructure-as-a-Service (IaaS) is the capability to provision processing, stor-age, networks, and other fundamental computing resources; the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, stor-age, deployed applications, and possibly limited control of some networking components, such as host firewalls. Services offered by this delivery model include: server hosting, Web servers, storage, computing hardware, operating systems, vir-tual instances, load balancing, Internet access, and bandwidth provisioning. The IaaS cloud computing delivery model has a number of characteristics, such as the fact that the resources are distributed and support dynamic scaling, it is based on a utility pricing model and variable cost, and the hardware is shared among multiple users [4]. This cloud computing model is particulary useful when the demand is volatile and a new business needs computing resources and does not want to invest in a computing infrastructure or when an organization is expanding rapidly.

C. The Carrier

It is an intermediary that provides connectivity and transport of cloud services.

D. The Broker

It is an entity that manages the use, performance, and delivery.

E. An Auditor

It is a party that can conduct independent assessment of cloud services, information system operations, performance and security.

III. Transparent Cloud Protection System (TCPS)

TCPS is a protection system for clouds aimed at transpar-ently monitoring the integrity of cloud components. TCPS is intended to protect the integrity of guest Virtual Machines (VM) and of the distributed computing middleware by allow-ing the host to monitor guest VMs and infrastructure compo-nents. TCPS is a middleware whose core is located between the Kernel and the virtualization layer. By either actively or passively monitoring key kernel or cloud components [3]. TCPS can detect any possible modification to kernel data and code, thus guaranteeing that kernel and cloud middleware integrity has not been compromised and consequently no attacker has made its way into the system. All TCPS modules reside on the Host and Qemu is leveraged to access the guest.

Suspicious guest activity can be noticed by the Interceptor and they are recorded by the Warning Recorder into the Warning Queue where the potential alteration will be evaluated by the Detector component [6]. TCPS can locally react to security breaches or notify the distributed computing security components of such an occurrence. In order to avoid false positives as much as possible, an administrator can notify TCPS of the new components' checksum.

IV. Client Based Privacy Manager

Client based privacy manager helps to reduce the risk of data leakage and loss of privacy of the sensitive data processed in the cloud, and provides additional privacy related benefits.

Fig.2. shows the overall architecture of the privacy manager. The main features of the privacy manager are:

- Obfuscation: This feature can automatically obfuscate some or all of the fields in a data structure before it is sent off to

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

the cloud for processing, and translate the output from the cloud back into de-obfuscated form. The obfuscation and de-obfuscation is done using a key which is chosen by the user and not revealed to cloud service providers [2].

- Preference Setting: This is a method for allowing users to set their preferences about the handling of personal data that is stored in an unobfuscated form within the cloud. This feature allows the user greater control over the usage of his data and makes it easier to handle and work with.
- Data Access: The Privacy Manager contains a module that allows users to access personal information in the cloud, in order to see what is being held about them, and to check its accuracy. This is an auditing mechanism which will detect privacy violations once they have happened.
- Feedback: The Feedback module manages and displays feedback to the user regarding usage of his personal information, including notification of data usage in the cloud. This module could monitor personal data that is transferred from the platform.
- Personae: This feature allows the user to choose between multiple personae when interacting with cloud services thus securing the personal information

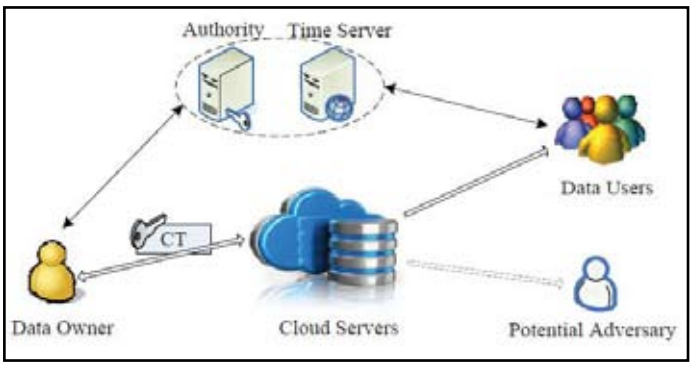

Fig. 2 : Client Based Privacy Manager [2]

V. Conclusion

In this paper, the importance of Encryption and Decryption of data, open security architecture of cloud Computing and the theory of cloud computing services viz. SaaS, PaaS, IaaS is discussed. Since Data privacy has become increasingly important in our litigious and online society, a new approach (KP-TSABE) is used for protecting data privacy from attackers who retroactively obtain through legal or other means is studied and analyzed. Also a novel aspect of our approach having essential properties of modern P2P systems, including churn, complete decentralization and global distribution under different administrative and political domains is mentioned.

VI. Acknowledgment

We wish to thank and express our deep sense of gratitude to our guides Prof. Deepali B. Gothawal and Prof. Vishakha A. Metre for her consistent guidance,inspiration and sympathetic attitude. Lastly we wish to thank the researchers for their contributions because of which we could complete this work.

References

[1] B. Wang, B. Li, and H. Li, Oruta: Privacy-preserving public auditing for shared data in the cloud, Cloud Computing, IEEETransactions on, vol. 2, no. 1, pp. 4356, 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. 282304, 2014.

[3] J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen, A full lifecycle privacy protection scheme for sensitive data in cloud computing, Peerto- Peer Networking and Applications.

[4] P. Jamshidi, A. Ahmad, and C. Pahl, Cloud migration research: A systematic review, Cloud Computing, IEEE Transactions on,vol. 1, no. 2, pp. 142157, 2013.

[5] 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. 4650, 2014.

[6] X. Liu, J. Ma, J. Xiong, and G. Liu, Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data, International Journal of Network Security, vol. 16, no. 4, pp. 351357, 2014.

[7] A. Sahai and B. Waters, Fuzzy identity-based encryption, in Advances in Cryptology EUROCRYPT 2005, ser. LNCS, vol. 7371. Springer, 2005, pp. 457473. [8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in Proceedings of the 13th ACM conference on Computer andCommunications Security. ACM, 2006, pp. 8998.