Volume 3, Issue 2, February 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Cloud Computing Privacy Solutions

Kalimullah Lone*
Department of computer science & Engg.
Lovely Professional university
India

Md. Ataullah
Department of computer science & Engg.
Lovely Professional university
India

Abstract— Cloud computing allows data and services to be placed in a pool of resources. The clients are able to access the resources of the cloud through service providers. The flow of these resources takes place through a common channel i.e. internet. The common channel makes it vulnerable to attacks. These attacks result in the privacy issues thus decreasing the level of trust of the customer on the cloud service provider. There are several solutions to solve these privacy related problems. In this paper we will describe cloud computing architecture and several methods to solve the privacy issues. We have analyzed each proposed solution with their pros and cons.

Keywords— Trusted Third Party, Set Top Box, Personal Identity Information, Identity Management.

I. INTRODUCTION

Cloud computing is the latest technology in computer science. It is the future of the computing. Cloud computing has been defined by National institute of standards and technology (NIST) as:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The important thing about cloud computing is that it provides essential characteristics, different services and has different models. Cloud computing centralizes all the resources on to the cloud. The users have to access the cloud to get the services. We assume that all the services which a user needs are present on the cloud. The user will be provided with all the software's, processors for computation, memory, network bandwidth and also with a storage, which a user needs. In return the users have to pay for the services on the monthly or weekly basis. The usage of resources may be pay by use or pay per cycle or the application may be accessed for few minutes or hours or users can access the resources for long term basis. Today, clients are capable of running their software applications in remote clouds where data storage and processing resources could be acquired and released almost instantaneously. In spite of all the advantages delivered by cloud computing, several challenges are hindering the migration of customer software and data into the cloud. On top of the list is the security and privacy concerns arising from the storage and processing of sensitive data on remote machines that are not owned, or even managed by the customers themselves.

Due to the problem of security and privacy, there are various solutions proposed to solve these issues. In this paper we will describe the architecture of cloud computing, analyse the privacy solutions and identify their pros and cons.

The rest of the paper is organized as follows. In section II problems existing in the cloud are described. It includes architecture of cloud computing and various attacks. Section III describes the existing solutions. Section IV shows the comparison of various solutions and section VI concludes the paper.

II. PROBLEM DEFINITION

A. Cloud computing architecture

The information stored locally on a computer can be stored in the cloud, including word processing documents, spreadsheets, presentations, audios, videos, records, financial information, appointment calendars etc. These all services are maintained on behalf of the cloud users by a cloud service provider. Cloud service provider manages and operates the storage and computing services [1]. The cloud customer uses the cloud storage and computing services remotely to store and process the data. The architecture of the cloud is shown in figure 1. The basic mechanism used in the cloud is demand and supply relations in the cloud marketplace. CPA and CAA are used to provide infrastructure and services to the users. Service providers are the entities used to understand the needs of a particular business and they provide service applications to the users. Service providers do not have computational resources for the applications; instead, they lease resources from infrastructure providers. Infrastructure providers provide them with seemingly infinite pool of computational, network and storage resources. Infrastructure providers operate host sites that have their physical infrastructure on which application are executed. Number of such sites form a marketplace [1].

Resources of the physical hosts are virtualized. They appear as multiple physical Machines to run multiple operating systems and applications. Cloud platform provides virtualized resources like computing power, memory, storage and bandwidth. Server virtualization is the process of running heterogeneous operating on the same physical server.VM monitor or hypervisor is used for the purpose of server virtualization [1]. The main channel through which traffic flows is

internet. The traffic flow through this channel leads to the security and privacy issues. There are various attacks possible to the traffic that flows through internet.

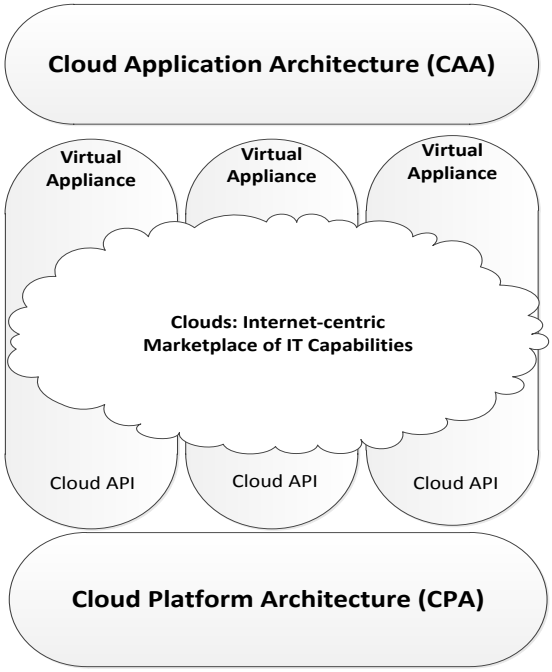

Figure 1: Cloud Computing Architecture

B. Cloud Computing Attacks

Most of the companies are moving towards cloud computing to make use of the services and applications. The attackers are also targeting cloud to get useful information. Some of the attacks are discussed below:

1) *Side channel attacks:* It is a type of attack in information is gained from the physical implementation of the cryptosystem rather than brute force attack. The attacker places a malicious virtual machine near the target cloud server and then performs the attack.

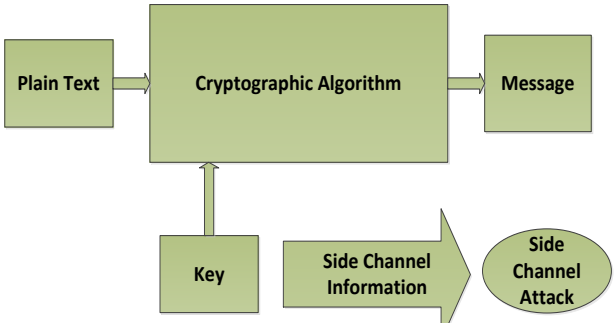

Figure 2: Side Channel Attack.

2) *Denial of service attack:* It is a type of attack in which a network is brought to its knees by flooding it with useless packets. The main purpose of this attack is making the machine resources unavailable to its intended users. When the cloud computing operating system notices large amount of workload due to DOS attack, it will provide more computational power to cope this extra workload. Since the damaged server is using the computational power of the main server, thus the increase in the computational power of the user will also affect the server.
3) *Authentication Attacks:* Most of the service providers use username and password for authentication purpose. Some financial organizations are exception to this procedure; they also add some shared secret questions, virtual keyboards etc. to make the authentication stronger. The attackers use phishing technique to perform the attack.
4) *Man in the middle attack:* This attack takes place when the attacker places himself between two users. The attacker modifies the data shared between the two users as shown in figure 2.

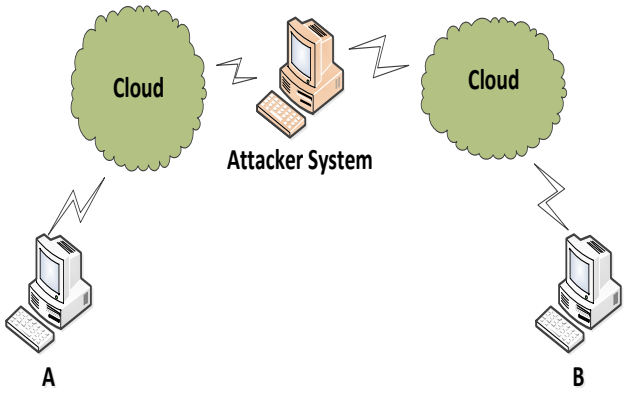

Figure 3: Man in the Middle attack

A. Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures

Waseem et al. [2] used the concept of cryptographic coprocessors to provide secure and isolated processing containers in the computing cloud. A cryptographic coprocessor is a small hardware card that interfaces with a main computer or server, mainly through a PCI- based interface. It is a complete computing system that is supported with a processor, RAM, ROM, backup battery, non-volatile persistent storage, and an Ethernet network card. The main responsibility of the TTP is to load a set of private/public key pairs into the persistent storage of the crypto coprocessor. Every public/private key pair is to be allocated to a single customer when the latter registers with the cloud privacy service. Upon registration, the cloud customer will securely receive a copy of her public/private key pair.

It provides temper proof casing to the crypto coprocessor which leads to the secure capabilities and makes it resistant to the physical attacks. A secure coprocessor tamper-resistance or tamper-responding mechanisms should reset the internal state of the coprocessor (RAM, persistent storage, processor registers) upon detecting any suspicious physical activity on the coprocessor hardware.

It also provides privacy to highly sensitive and normal data. Data marked with no privacy attribute will be stored without any form of encryption. Data marked with privacy using trusted provider attribute is encrypted by a specific provider key. Data marked with privacy using non trusted provider is encrypted on the customer side by customer specific key. Thus customers have the flexibility to store data on the basis of sensitivity.

Customers have to manage large number of accounts of different service providers. To remember the login information of these service providers and to keep a watch on the expiry of these services is a difficult job.

B. Privacy enhanced Cloud Services Home Aggregator

Sanvido et al. [3] used the concept of Set top box (STB), which guarantees privacy for end user's data and operations. Single software is installed in the home STB, as a single point of concentration for user's Cloud service accounts. High degree of privacy is achieved by splitting user's data and operations over multiple accounts and even over multiple providers. Accounts belonging to different providers, would require inter provider collaboration to perform an attack. Privacy enhanced storage is achieved by extending the very simple architectural design of the Cloud service aggregator.

This method takes care of all service providers and services subscribed by the customer. The account details and the validity of the services are also maintained by the set top box.

The set top box cannot be used in all the computing devices because of the portability issues. The device is fixed at a place and cannot be moved from place to place.

C. Protection of Identity Information in Cloud Computing without trusted Third Party

Ranchal et al. [4] implemented the privacy mechanism by using the authentication without trusted third party. The cloud service provider (SP) is a third party that maintains information about or on behalf of another entity. Trusting a third party requires taking the risk of assuming that the third party will act as it is expected. Whenever some entity stores or processes information in the cloud. Privacy or confidentiality question may arise. Two type of problems are addressed:

1) *Authenticating without disclosing Personal identity information (PII)*: when a user sends PII to authenticate for a service, the user may encrypt it. However, PII is decrypted before a service provider (SP) uses it. As soon as PII is decrypted, it is prone to attacks.
2) *Using services on untrusted hosts*: The available Identity management (IDM) solutions require user to execute IDM from a trusted host. They do not recommend using IDM on untrusted hosts, such as public hosts.

The paper has proposed an approach for IDM in cloud computing that does not require TTP , can be used on untrusted or unknown hosts and uses encrypted data when negotiating the use of PII for authentication to services in cloud computing. The scheme has used active bundles (sensitive data) for IDM. An active bundle is sent from a source

host to a destination host. The information is compared and upon verification the users are provided access to the services. Verification of the users on the basis of IDM will provide attackers an opportunity to mislead the users through masquerade.

D. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing

Qian et al. [5] proposed a scheme for the security and privacy which uses a trusted third party system. It also enables public audit ability and data dynamics for storage security in cloud computing. The components of the scheme are client, cloud storage server and third party auditor. The two main issues in this scheme are key generation (KeyGen) and Signature Generation (SigGen). The client computes signature for each block. The client then generates a root R based on the construction of the Merkle Hash Tree, where the leave nodes of the tree are an ordered set of hashes of "file tags". Next, the client signs the root "R" under the private key. The root metadata R has been signed by the client and stored at the cloud server, so that anyone who has the client's public key can challenge the correctness of data storage. Various operations performed by this scheme efficiently are data modification (M), data insertion (I), and data deletion (D) for cloud data storage.

Integrity verification can be easily performed. Upon receiving the response from the prover, the verifier generates the root of the merkle hash tree and authenticates it by checking. After performing operations like insertion, modification and deletion, the tree is reorganized to maintain the order.

The restructuring of the tree seems to be easy but it is difficult to maintain the order and position of every node after the operation is performed.

E. Ensuring Data storage security in cloud computing

Wang et al. [6] proposed Privacy preserving public auditing for secure cloud storage. The concept used is trusted third party system. To fully ensure the data integrity and save the cloud users computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third party auditor (TPA) to audit the outsourced data when needed. The TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. Insertion, deletion, updating, file retrieval, error recovery and append operations are handled through array operations.

The main function performed is public auditing and it consists of two phases:

1) Setup: The user initializes the public and secret parameters of the system by executing key generation (KeyGen), and Pre processes the data file F by using signature generation (SigGen) to generate the verification metadata. The user then stores the data file F and the verification metadata at the cloud server, and delete its local copy. As part of pre-processing, the user may alter the data file F by expanding it or including additional metadata to be stored at server.
2) Audit: The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will derive a response message by executing GenProof using F and its verification metadata as inputs. The TPA then verifies the response via VerifyProof.

F. Data security in the world of cloud computing

Harauz et al. [7] proposed a scheme for the data security to ensure data confidentiality, integrity, and availability (CIA). The storage provider must offer capabilities that a tested encryption schema must ensure that the shared storage environment safeguards all data. Stringent access controls are provided to prevent unauthorized access to the data. It also provides scheduled data backup and safe storage of the backup media. To advance cloud computing, the community must take proactive measures to ensure security. A movement exists to adopt universal standards (open source) to ensure interoperability among service providers. Even though community at large is aware of the need for security and is attempting to initiate robust measures, a realm of security concerns transcends these efforts.

IV. COMPARISON OF EXISTING SLOUTIONS

From the description of each of the solutions presented in section III, we can easily notice that most of the attacks are not solved by any single existing solution.

The solutions based on the cryptography [2, 5, 6] have caused a problem to install a hardware chip on each machine. The use of extra hardware and to install it on every machine is difficult because every user has to take care of this extra burden. The use of set top box [3] has limited the domain of computing because it does not include mobile computing due to its portable nature. The use of a trusted third party [5, 6] provided a secure method to keep the data and resources secure, but the main problem is that there is always some data which a user never wants to disclose. So the use of trusted third party cannot be always trusted for securing the data. The use of authentication without third party [4] can be easily cracked through authentication attacks because most of them offer username and password to authenticate two users. We have compared all these existing techniques in table I.

Table I: Comparison of existing solutions

Existing Solutions	TTP	STB	Hash Function	Crypto-graphy	Efficient data retrieval	Mechanism
Waseem et al. [2]	Yes	No	No	Yes	No	Additional Coprocessor for privacy
Sanvido et al. [3]	No	Yes	No	No	No	Set top box
Ranchal et al. [4]	Yes	No	Yes	Yes	No	Authenticatio n without third party
Wang et al. [5]	Yes	No	Yes	Yes	No	Authenticatio n using third party
Wang et al. [6]	Yes	No	No	Yes	No	Authenticatio n and audit using third party
Harauz et al. [7]	No	No	No	Yes	No	Asymmetric key generation

V. CONCLUSIONS

This paper described cloud computing, its architecture, various attacks like side channel attack, denial of service attack, authentication attack and man in the middle attack. We have analysed various solutions; identified their strengths, limitations and provided comparison among them. So we say that this paper can be used as a reference by researchers when deciding the privacy issues in the cloud. We are also working on developing a new technique to make the services of the cloud easily available and also to make them private.

REFERENCES

[1] Huaglory Tianfield, "*cloud computing architecture*", 2011 IEEE.

[2] Wassim Itani and Ayman Kayssi, "*Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures*", 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[3] F. Sanvido, D. Díaz-Sánchez, R. Sánchez-Guerrero, F. Almenares and P. Arias, "*Privacy enhanced Cloud Services Home Aggregator*", 2012 international conference on ICCE.

[4] Rohit Ranchal and Lotfi Ben Othmane,"*Protection of identity in cloud computing without trusted third party*",2010 29 th international symposium on reliable distributed systems.

[5] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li , " *Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing*", IEEE ransactions on parallel and distributed systems, VOL. 22, NO. 5, MAY 2011.

[6] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, " *Privacy-Preserving Public Auditing for Secure Cloud Storage*", 2011 IEEE.

[7] Lori M. Kauifman," *Data Security in the World of Cloud Computing*", JULY/AUGUST 2009, COPublished by the IEEE Computer and Reliability Societies.

[8] Jen-Sheng Wang and Che Hung Liu ," *How to manage information security in cloud computing*", 2011 IEEE.

[9] Cong wang and Qian wang , "*Ensuring data storage security in cloud computing*",2011 IEEE.

