International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876; Impact Factor: RJIF 5.44
Received: 27-06-2019; Accepted: 29-07-2019
www.newengineeringjournal.in
Volume 5; Issue 3; July 2019; Page No. 141-144

Privacy and security challenges in cloud: A review

Dr. Mukesh Singla
Professor, Sat Priya Institute of Engineering & Technology, Rohtak, Haryana, India

Abstract
Cloud computing is growing in popularity due to its ability to offer dynamically scalable resources provisioned as services regardless of user or location device. However, moving data to the cloud means that the control of the data is more in the hands of the cloud provider rather than the data owner. This is a great challenge that continues to hinder cloud computing from successfully achieving its potential. This is due to the fact that with cloud computing, the storage and processing of private information is done on remote machines that are not owned or even managed by the cloud consumers. This brings about significant security and data privacy concerns that impede the broader adoption of cloud computing, which compromises the vision of cloud computing as a new IT procurement model.

Keywords: information technology, cloud service provider, trusted platform module, trust computing, service level of agreement

1. Introduction

Clouds are the new technologies in development of the distributed system being grid as its predecessor. The cloud provides abstraction of its services, so no expertise or knowledge regarding it is needed by the users. Higher computing power, high scalability, higher quality of service and higher throughput are achieved by the usage of internet services. High speed internet is needed to access the online business applications being provided by the cloud providers [1].

1.1 Privacy and security challenges

Cloud computing services depend mainly on virtualization, web application and provide ubiquitous network access to its customers, since cloud facilities are retrieved via the network using the standard network protocols. This network is mainly internet which is well known for being untrustworthy. Web application implements session handling and various session management operations are susceptible to meeting ridding and session hijacking while HTTP by nature is a stateless protocol whereas web application itself requires certain concept of session state [2].

The skilled hacker may successfully escape from the virtualized environment and inflict harm on the cloud infrastructure by altering some configuration settings and gaining access to restricted system. The on-demand cloud characteristic is achieved through the management interface. The interface is accessible to cloud service users and is vulnerable, given that authorized access to management interface is bound to take place in cloud systems.

This is contrary to traditional systems, in which the management interface is only accessible to limited system administrators. The management interface is also realized using web application so it repeatedly shares the vulnerability of web application, and it can also suffer from denial of service attacks since the most common authentication method is that of password and username which locks the user out after several unsuccessful attempts [3].

Resource sharing by cloud consumer presents a situation whereby bits of data can be recovered from the last consumer who was using the resource. This is owing to the cloud computing characteristic of resource pooling, which entails that cloud resources are relocated to the next available users once the one who was using it is done with it. In case of adversary attacks and breaking through the encryption of a database operated by a CSP in a multi-tenant service, chances are that attacker might have the capacity to take the information of handfuls or several diverse business buyers put away on that database.

Cryptographic techniques are generally used by cloud computing service providers to solve security related problems. Whoever, cryptanalysis advances day by day and they can easily render a well-known cryptographic algorithm insecure when a flaw is discovered in the algorithm. This imperfection is cast-off by the committers to go what used to be a robust encryption into a fragile encryption or, no encryption at all, since more methods of breaking cryptographic mechanisms are often discovered.

The issue of poor key management is also a very troubling challenge. A study conducted by the European network and information security agency revealed that cloud computing infrastructure requires management and storage of many different kinds of keys as a result of many virtual machines. These vulnerabilities in core cloud computing technologies are the main contributing factor to customers’ reluctance to move into the cloud.

1.2 Trusted Platform Module (TPM)

Trusted Computing Group, 2010 and MIMOS, 2012 developed standards for hardware enabled trusted computing, TPM is a hardware security component was then formulated and built into many computers and computer-based products (Abadi, 2004; MIMOS National R&D Centre in ICT, 2012; Trusted Computing Group, 2010). According to Morris, (2011) the chip allows for machine authentication, hardware encryption, signing, secures key storage and attestation. TPM monitors, software as it is loaded and provides secure reports on exactly what is running on the machine.

The major advantage of using this chip is that it generates evidence-based confidence that every claim made by the cloud service provider concerning the security of its infrastructure is legitimate. Having gained this kind of trust, the customer feels at ease to outsource any kind of information while it reaps an even more lucrative pay-out. According to Kleyman, (2012) this chip does not protect against attacks that exploit security vulnerabilities introduced by the programming bugs. Furthermore, TPM does not protect the hardware from its owner, but only for its own, leaving the door wide open for insider threat such as rogue administrators.

1.3 Trusted Computing (TC)

The IT community, particularly the Trusted Computing Group (TCG), is attempting to build a set of technologies, e.g., authentication, data encryption, identity and access management, password management, network access control, and disaster recovery, to provide assurance that computer systems will fulfill the desired way of operation [4]. The TCG applies the trusted computing scheme to the Trusted Multi-Tenant Infrastructure (TMI) to establish trust in an un-trusted environment such as in a public cloud computing service. The new concept aims to enable clients to assess the trustworthiness of cloud providers by applying a set of hardware and software technologies. The remote server attestation is one of these technologies that allows clients to attest hosts [2]. The TCG starts building their solutions based on establishing a standard hardware module, the Trusted Platform Module (TPM), which carries out basic cryptography functions such as the hash function and RSA. These cryptography functions are required to establish a trust state in a computing hardware [5, 6]. In other words, the TCG aims to provide standard hardware and software technologies for trusted computing including cloud computing. Therefore, several of the security solutions, particularly those proposed to secure virtual isolation between VMs and a VM from the server provider, are based on TC technologies [7, 8, 6]. These technologies still face several challenges and cannot be used solely to provide a universal solution to all cloud security problems [16]. For instance, if the TPM, which is the core component of TC, is compromised, the entire solution will be affected as pointed out by Christopher Tarnovsky in 2010 [10]. In addition, the TC concept does not provide the cloud users enough control of their data in terms of privacy and security policies. Trust is always a worry for the new technologies and also for distributed computing paradigm

2. Protecting data privacy and integrity from cloud providers

Privacy and integrity are important requirements for various applications such as e-government and EHR (Electronic Health Record) [39]. Cloud computing customers are not only worried about the compromising of privacy and integrity of their data from possible attackers, but also from potential curious cloud providers.

Unfortunately, security breaches counted in 2011 and listed in show that big companies such as Google, EMC/ RSA, Sony, UK National Healthcare System (NHS) and Amazon EC2 all experienced security incidents. In cloud computing, customers' data are outsourced to cloud providers which can be either trusted or untrusted. The term un-trusted may be used to indicate that the cloud providers cannot be fully trusted. For instance, un-trusted cloud providers may not alter users' data but they can passively compromise data privacy or stealthily change the protocols for their financial benefit [38]. In other words, a cloud provider server can be considered as a honest-but-curious server [10]. Hence, it is trustworthy in providing the services, in terms of data availability, enforcing basic security control requirements and processing honestly authorized queries on stored data and returning the correct results. Nevertheless, possible malicious actions from inside the cloud can be carried out from a malicious administrator or employee.

Toward the more widespread adoption of cloud services, researchers are investigating and developing novel techniques that preserve privacy and integrity of outsourced data without fully depending on the cloud providers to provide these security requirements. The solutions should provide customers more control over the protection of their data and protect the data from the providers as well [7]. As a cloud provider server hosting outsourced data may not be fully trusted, several researchers (e.g. [12, 13-14] have proposed methods to deal with this kind of situations. In general, their proposed solutions are based on encrypting data before the data are sent to the cloud provider server.

Although encrypted data are secured from unauthorized access, the encrypted data cannot be fully useful unless they are decrypted. For example authorized users cannot search for keywords in the encrypted data, use the encrypted data as input to computation or comparison operations. Because decrypting data at the cloud may possibly expose its content to the provider servers at least, it is more secure to decrypt data only in trusted machines controlled by the user who is authorized to access these data.

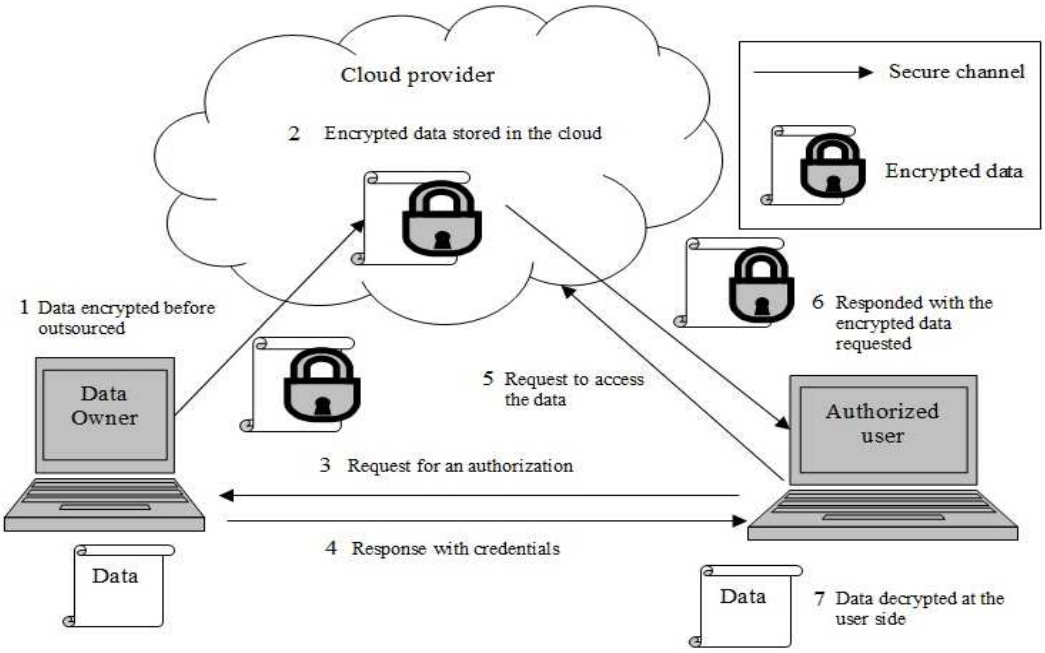
Cloud provider
2 Encrypted data stored in the cloud
Secure channel
Encrypted data
1 Data encrypted before outsourced
Data Owner
5 Request to access the data
6 Responded with the encrypted data requested
Authorized user
3 Request for an authorization
4 Response with credentials
Data
Data
7 Data decrypted at the user side

Fig 2.1: Basic architecture for preserving data privacy in the cloud

Figure 2.2 shows the basic architecture of encrypting data for privacy protectionbefore sending it to the cloud. Then the data remain encrypted in the cloud and only users authorized by the data owner can get the credential for accessing the encrypted data. The encrypted data can be decrypted only after they are downloaded to an authorized user machine. In such a scenario, the privacy of the data does not depend on an implicit assumption of trust of the server or of the service level of agreement (SLA). Instead, the protection of privacy depends on the encryption techniques used to protect the data [15]. The remaining issues are how to allow the data owner and authorized users to share and search the encrypted data, and use them for some computations, according to their access rights. All these functions should be done in a secure manner without exposing any private information to unauthorized entities including cloud providers. New cryptography techniques, trusted computing schemes and information centric security approaches [2] can be the promising solutions to overcome several cloud computing security challenges.

2.1 Cryptography techniques fitting the cloud model

New cryptography technologies are required to fit the cloud model and to increase data security with less impact on its usability. For example, searchable encryption [3] is one area where researchers develop the capability of search of encrypted data without decrypting it. Only authorized users can query and retrieve encrypted data without exposing any private information either about the data or the query which may contain information about the data [46]. Another example is encryption techniques that enable computation operations of encrypted data without decrypting them. In such techniques, the results from the computation, which usually contain information about the protected data, are also protected. An example of these techniques is Homomorphic encryption [3]. There are other cryptography techniques such as Identity Based Encryption (IBE) and Attribute Based Encryption (ABE) [16] that can improve key management and access control of cloud systems.

3. Conclusion

Data security and privacy challenges are the most cited substantial obstacles to the broader adoption of cloud computing technology across the globe. This owes to the fact that cloud computing acts as a big black box, making it close to impossible for its client to know what is going on within.

Despite the benefits that the cloud presents, cloud computing technology is faced with a variety of legal and technological challenges. Security and privacy are amongst the major challenges as identified in the literature. These challenges are attributed to the lack of proper security control policies and weaknesses in security safeguards in cloud deployments. The rampant accidental and deliberate data breaches have become synonymous with the cloud and have led to a widespread recognition of the privacy risks in cloud deployments.

4. References

1. Tari Z, X Yi, Premarathne US, Bertok P, Khalil I. "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges," in IEEE Cloud Computing. 2015; 2(2):30-38. doi: 10.1109/MCC.2015.45
2. Ali M, Revathi Dhamotharan, Eraj Khan. SeDaSC Secure Data Sharing in Clouds, in IEEE Systems Journal. 2017; 11(2)395-404. doi: 10.1109/JSYST.2014.2379646
3. Subha T, Jayashri S, Efficient privacy preserving integrity checking model for cloud data storage security, Eighth International Conference on Advanced Computing (ICoAC), Chennai, 2016-2017, 55-60. doi: 10.1109/ICoAC.2017.7951745
4. Yong Yu, Liang Xue, Man Ho Au, Willy Susilo, Cloud data integrity checking with an identity-based auditing mechanism from RSA, Future Generation Computer Systems, Volume 62, September, 2016, 85-91.
5. Sakthivel S, Dhiyanesh B. A privacy-preserving storage security for spatial data in dynamics cloud environment, Fourth International Conference on Computing,

Communications and Networking Technologies (ICCCNT), Tiruchengode, 2013, 1-6. doi: 10.1109/ ICCCNT.2013.6726759

6. Subha T, Jayashri S. Efficient privacy preserving integrity checking model for cloud data storage security, 2016 Eighth International Conference on Advanced Computing (ICoAC), Chennai, 2017, 55-60. doi: 10.1109/ICoAC.2017.7951745
7. Zawoad S, Dutta AK, Hasan R. Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service, in IEEE Transactions on Dependable and Secure Computing. 2016; 13(2):148-162. March-April 1. doi: 10.1109/TDSC.2015.2482484
8. Alabool HM, Mahmood AK, Common Trust Criteria For IaaS cloud evaluation and selection, 2014 International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, 2014, 1-6. doi: 10.1109/ICCOINS.2014.6868444.
9. Hassan Rasheed. Data and infrastructure security auditing in cloud computing environments, International Journal of Information Management. 2014; 34(3):364-368
10. Stephen Pritchard, Security in the clouds, Infosecurity. 2009; 6(1):34-37.
11. Jie Zhu, Guoyuan Lin, Fucheng You, Huaqun Liu, Chunru Zhou. Multiway dynamic trust chain model on virtual machine for cloud computing, in China Communications. 2016; 13(7):83-91. doi: 10.1109/CC.2016.7559079
12. Mackay M, Baker T, Al-Yasiri A. Security-oriented cloud computing platform for critical infrastructures, Computer Law & Security Review. 2012; 28(6):679-686.
13. Tianfield H. Security issues in cloud computing, IEEE International Conference on Systems, Man, and Cybernetics (SMC), Seoul, 2012, 1082-1089. doi: 10.1109/ICSMC.2012.6377874.
14. Sokratis K. Katsikas C. SEPRICC Security and Privacy in Cloud Computing proceeding of The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 2012,
15. Galis A, Gavras A. (Eds.) FIA, LNCS 7858, 2013, 153-158.
16. Irfan Hussain. Security Issues in Cloud Computing - A Review, Int. J. Advanced Networking and Applications. 2014; 6(2):2240-2243. ISSN: 0975-0290