IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 10-14
www.iosrjournals.org

Data Centric Security Approach: A way to Cloud Computing Security & Privacy

Prof. Pooja Shelke[1], Dr. Asish Sasankar[2]
[1](poojashelkeifsc@gmail.com , MCA, TGPCET/ RTMNU, India)
[2](ashish.sasankar@raisoni.net , MCA, GHRIT/ RTMNU, India)

Abstract: *Cloud computing paradigms are gaining widespread acceptance due to the various benefits they offer. These include cost-effectiveness, time savings and efficient utilization of computing resources. However, privacy and security issues are among the major obstacles holding back the widespread adoption of this new technology. Some research is focused on improving the security at the application, operating system, Virtual Machine (VM) or hardware levels. These solutions do not normally provide a comprehensive solution and they still keep the data security measures under the control of the cloud provider. Another direction of research is based on Trust Computing (TC) concepts. In essence, these provide a set of trusted third party technologies to secure the VM from the cloud provider. While these approaches provide the users with tools to monitor and assess the security aspects of their data, they do not provide the users with much control capability. In contrast, Data Centric Security (DCS) is an emerging approach that aims to provide data owners with full control of their data security from within the data itself, throughout the data's lifecycle on the cloud. However, the concept of the DCS approach is interpreted in various ways in the literature and there is not yet a standardized framework of applying this approach to the cloud model.*

Keywords - *DCS, Trusted Computing, Data Security.*

I. INTRODUCTION

The DCS concept is based on providing security at the data level. Hence, the data are self-describing, self-defending and self protecting during their lifecycle in the cloud environments. The data owner is solely responsible to set and manage the data privacy and security measures. These requirements can be achieved without depending on trusting the cloud provider or/and a trusted third party assistance. Then, this conceptual framework is developed into an applied solution. The proposed solution is based on the Chinese Remainder ix Theorem (CRT) and utilizes symmetric and asymmetric encryption techniques. To reduce the computational and management overheads, access control policy enforcement and sharing the symmetric key of encrypted data are accomplished in an efficient manner based on the CRT. For enhancing security, the data owner is able to use a unique symmetric key for encrypting each set of data and to attach it securely to the encrypted data. Only authorized users are given access to the key. Additionally, the privacy of access is improved by keeping the number of authorized users and their identities hidden even from the cloud provider. Moreover, secure search capabilities on the encrypted data are an integral part of the proposed solution. All the required security parameters, including integrity and authenticity proof parameters, are attached to the encrypted data to create a secure file container, which is referred to as a DCS file. Only authorized users can search and access DCS files, based on the embedded policies that are set and managed exclusively by the data owner.

II. TRENDS & DIRECTIONS TO CLOUD COMPUTING SECURITY

Cloud computing technology faces different challenges that cannot be addressed directly by traditional solutions. A suitable solution should adapt to the specific characteristics of this new computing paradigm. The research directions of addressing cloud computing issues are various according to which kinds of cloud problems the researchers focus on. At the virtualization level of the technology, it is claimed that issues related to the isolation between VMs in the same physical machine need more attention in terms of security and performance [33]. Paper [11] claims that the major issues of cloud security centre around cloud infrastructure, software platform and user data, in addition to related issues of access control, identity management and data integrity without neglecting the physical security of data centre and processes. However, it can be claimed that the privacy and integrity of data are the essential security requirement particularly in un-trusted clouds. Also in trusted or partially trusted clouds, a strong privacy mechanism can be the key for establishing trustworthiness. An un-trusted cloud server can expose customers' private data and activity patterns, and return incorrect data from computational processes to customers. It is also possible that an un-trusted provider can manipulate the legitimate way of handling users' requested operations to their advantage [38]. Therefore, protecting data,

particularly its privacy and integrity, from both the cloud providers and external attackers, is expected to result in stronger cloud security architectures that encourage wider adoption of cloud services.

III. PROTECTING DATA PRIVACY 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 [21] 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 [40]. 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. 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.
Figure 1.1 shows the basic architecture of encrypting data for privacy protection before 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 [45]. 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 [11] can be the promising solutions to overcome several cloud computing security challenges.

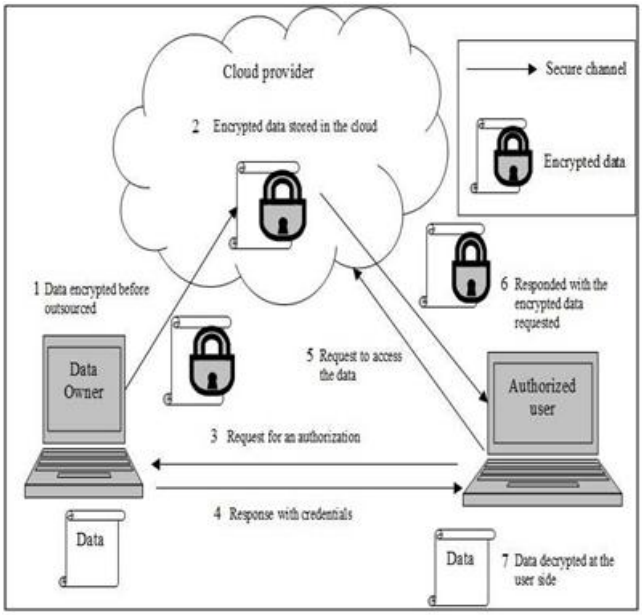

Fig 1.1- Basic Architecture for preserving data in CC

III DATA CENTRIC SECURITY (DCS)

In traditional techniques of protecting data, security is provided by the server which stores the data. The methods used to protect the data as well as management of the protected data are controlled by the

administrators of the server. This kind of approach can be classified as a system-centric approach, which is not suitable for protection of clients 'data in the less trusted cloud environment. A data centric approach is expected to be more effective and adaptive for cloud services [20, 41, and 51]. The term data centric security indicates in general that the focus of the security protection is around the data. This terminology can be used differently. For cloud computing, the approach of data centric security is to secure data from the inside so that the data, according to their value and classification, have their security requirements built in to the actual data to provide optimal data security at any stage of the data life time, regardless of the environment where the data are stored [23].

In cloud computing, customers' data are stored mostly in virtual storages in a cloud service provider's cloud infrastructure. In the public SaaS and DaaS models, customers only own the stored data while all the hardware and software involved in storing and processing of the data are owned by the service providers. In other models such as the public IaaS and PaaS models, software handling of the data and applications is also owned by the customers, while the hardware is not. Therefore, from the cloud customers perspective, the most valuable asset in the cloud environment is their data, specifically data that contain sensitive information such as government, healthcare, and financial data**.** With the benefits offered by the use of cloud computing, customers who used to store their sensitive data in a secure private computing environment become increasingly attracted to outsourcing their sensitive data to the cloud.

The traditional security concept ordinarily centres around the technologies and devices used to store and handle data. This concept can be difficult to be adapted to provide the appropriate security level required particularly for sensitive and confidential data [23]. Though cloud security and privacy have recently drawn the attention of the research community, proposed solutions have mostly focused on securing the underlying Operating Systems (OSs) and Virtual Machines (VMs) that host cloud services [9, 16, 17, 19, 52-54]. Hence, most solutions are still based on the traditional security concept and most focus on either system-centric or VM centric security [22]. Some of these solutions are based on the Trusted Computing (TC) concept which is introduced and developed by the Trusted Computing Group (TCG). The TCG aims to develop a set of technologies and standards, such as Trusted Platform Module (TPM), and blind processing and self-encrypting drive technologies, which can keep the clients data and applications handled within the cloud hardware in a claimed trusted secure container which is secured even from the cloud system administrators [15, 16]. The TCG, based on their technologies, focuses on providing a set of tools which can be used to assist the cloud users to evaluate the trustworthiness of cloud providers, monitor compliance to policy, and enable transparency regarding the physical location of data in the cloud [55]. However, the cloud users have to trust the TCG technologies first in terms of assessing the trustworthiness of the cloud provider and if the TPM, which is the basic component to build this trust, gets compromised, the entire solution will be affected.

In 2010, Christopher Tarnovsky claimed that he had succeeded in compromising the TPM [50]. Consequently, research and proposed solutions based on the TPM may need to be re-evaluated. Even if the TPM and other TCG tools are security assurance, the focus of these tools is not on providing users with the desired control of the security and privacy of their data. Instead, from a customers perspective, an implementation of the TC concept allows customers to monitor or audit the operations, including access control policies, of the cloud server through trusted tools that can provide proof of compliance to the TC concept to the users [20]. A new concept has been suggested by several researchers for addressing the specific security issues of cloud computing by shifting the focus of securing customer's data to the data itself and they call it Data Centric Security (DCS) or Information Centric Security (ICS) [11, 15, 20-23]. This concept is still developing and there are different views about how to apply it to the cloud model.

For a comprehensive security solution, all these three security classifications should be integrated and be adapted to the cloud model. However, the dependency of one level of security on that of another level must be minimised. For example, the security functions provided at the data-centric security level should not rely on the other security levels, particularly the VM (hypervisor) and hardware levels as these two levels, in the public cloud, are controlled by the cloud provider in all the cloud delivery models. Moreover, from the responsibility perspective, the security data centric security level must be managed only by the data owner as the data in the cloud are owned by the data owner regardless of which cloud model is hosting them.

In terms of investigating the diversity view of understanding the DCS (or ICS) concept, several researchers' description and understanding of the concept are listed in Table 3.1. The list also shows how the concept has been evolved over time by the IT research community.

In the DCS concept, data security solutions for the cloud computing paradigm can be classified based on two criteria:

The first classification is based on which level the security is provided at, and the second classification is based on who is responsible for providing the security. On the right-hand side of Figure 1.2, the levels that security functions can be provided at, in relation to data, are illustrated. In general, solutions focusing on providing security from outside the data level are classified as system-centric security. If the solutions focus on

a particular level, they are classified according to that specific level. For example, solutions that aim to improve the security isolation between VMs at the VM (hypervisor) level can be classified as VM-centric security solutions. On the other hand, solutions aiming to provide data security from within the data itself, as shown on the left-hand side of Figure 3.1, are classified as data-centric security solutions. The levels shown in Figure 1.2 are typical levels. There can be more or fewer levels in a practical system, based on the actual requirements and implementation. An example of the second classification is illustrated in Figure 1.3. There are three responsibility levels of security:

a. Service provider level where security is provided and sponsored by the cloud provider.
b. Trusted Computing level where security is provided and sponsored by a third party.
c. Data-centric security level where security is provided and sponsored by the data owner.

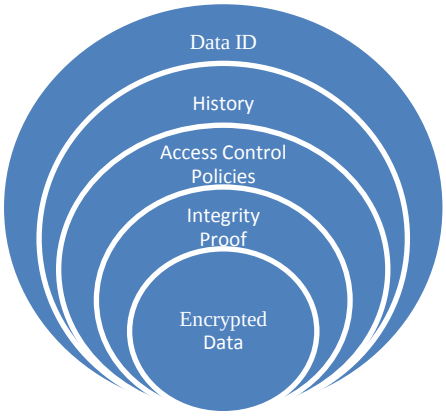

Fig:1.2 – Data Centric Security

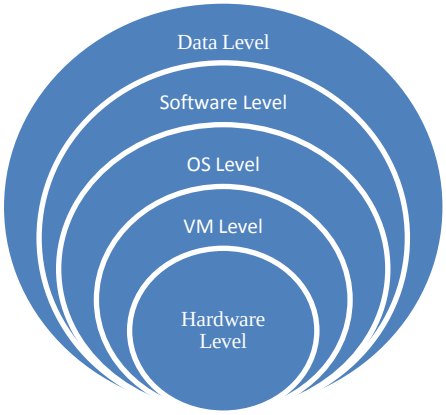

Fig:1.3 – System Centric Security

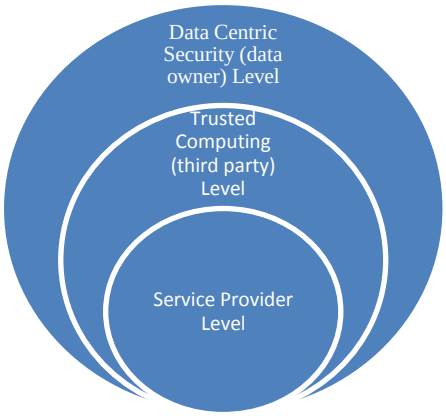

Fig:1.4 – Possible Security Levels in CC

When applying the DCS concept to a cloud computing system, the issue of securing the data from the cloud system itself is involved. Consequently, on the one hand, in some studies [21, 22, 56-58] the DCS concept is applied to the cloud while still focusing on providing the proper security level from the outside of the data and they attempt to protect their security mechanisms and secure the data from the cloud system that hosts the data based on the TC concept. On the other hand, in other studies [11, 20, 23, 59] the DCS concept for cloud computing is based on providing the security features from within the data, i.e., inside data, so it becomes self describing, self-protecting and self-defending. However, in [20], the DCS depends on TC technologies for assessing the environment trustworthiness hence the data security requires an outside data security measure. In [15] the data centric view of securing and preserving privacy of data in the cloud is presented by providing data confidentiality and privacy access to the data using either the TC approach or the DCS approach where data are self-protected. However, after the data have moved to the cloud the researchers are not agreed about what is responsible, i.e., the data owner, the cloud provider or the third party, for maintaining and managing data security under the data centric security concept.

REFERENCES

[1]. B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," Security & Privacy, IEEE, vol. 9, 2011, pp. 50-57.
[2]. T. Dillon, W. Chen, and E. Chang, "Cloud Computing: Issues and Challenges," in Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, 2010, pp. 27-33.
[3]. M. Malathi, "Cloud computing concepts," in Electronics Computer Technology (ICECT), 2011 3rd International Conference on, 2011, pp. 236- 239.
[4]. P. Mell and T. Grance. (2011, 7/8/2012). NIST Definition of Cloud Computing
[5]. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, 2012, , pp. 69-73,
[6]. S. Pearson, "Privacy, Security and Trust in Cloud Computing," Privacy and Security for Cloud Computing, 2012, pp. 3-42.
[7]. C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," Computers & Electrical Engineering, 2012.
[8]. T. J. Lehman and S. Vajpayee, "We've Looked at Clouds from Both Sides Now," in SRII Global Conference (SRII), 2011 Annual, 2011, pp. 342-348.
[9]. N. el-Khameesy and H. A. Rahman, "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems," Journal of Emerging Trends in Computing and Information Sciences, vol. 3, 2012.
[10]. W. Cong, W. Qian, R. Kui, and L. Wenjing, "Ensuring data storage security in Cloud Computing," in Quality of Service, 2009. IWQoS. 17th International Workshop on, 2009, pp. 1-9.