A Novel Data Security Model for Cloud Computing

Sh. Ajoudanian and M. R. Ahmadi

***Abstract*—Since the mid 1990's, the computational systems have changed from centralized to distributed model. Emergence of virtualization changes the system architecture to virtual centralization. On the other hand, in centralized computing, there is full control on data and processes where in virtual centralization the clients don't know where the data is stored and where the processes are running. In this architecture, security is a major concern especially in network, host, application, and data levels. For specific application for instance in cloud computing that is the major focus in this paper, data security is the main concern. Because of diversity in service models which are provided in cloud computing, achieving acceptable level of security is very important. These service models are Software as a Service, Platform as a Service and Infrastructure as a Service. We have proposed a novel data security model for cloud computing based on separation of security in different category layers. The proposed model certifies that our method can improve security levels in service oriented systems, especially in cloud computing applications.**

***Index Terms*—Cloud computing, data security.**

I. Introduction

The cloud computing operates from the idea that work done on the client side can be moved to some unseen cluster of resources on the Internet [1]. Cloud computing applies a virtual platform with elastic resources putting together by on-demand provision of hardware, software, and datasets, dynamically [2, 3]. Cloud computing leverages its low cost and simplicity to both providers and users [4, 5].

But the Internet is not a place that providers have complete control over it. Because of security concerns, cloud computing is not concerned with some users. As a virtual environment cloud computing has its special security threats and these threats are completely different from threats in physical systems. In this paper some security concerns in cloud computing especially data security are examined.

The reminding sections are organized as follows: In section 2, cloud service models and their security concerns are reviewed. Section 3 is examined data security models. Then in section 4, a new data security model for cloud computing is proposed, and finally in section 5, future works and results are discussed.

Manuscript received April 1, 2012; revised May 3, 2012.

Sh. Ajoudanian is with Computer Engineering Department, Islamic Azad University Science and Research Branch, Tehran, Iran (e-mail: shajoudanian@ pco.iaun.ac.ir).

M. R. Ahmadi is with Iran Telecom Research Center, Tehran, Iran (e-mail: m.ahmadi@itrc.ac.ir).

II. Cloud Computing Service Models and Their Security Concerns

In this section, cloud service models and their security concerns are discussed. Each service has its own security issues. These models are based on different SLAs that are between providers and users.

A. Software as a Service Model

In the SaaS model, the user buys a subscription to some software product, but some or all of the data and code resides remotely [1] and customers can access to this services via internet. In this model, applications could run entirely on the network, with the user interface living on a thin client.

With SaaS, users must rely heavily on their cloud providers for security [2]. Degree of control by providers is high and they are responsible for confidentiality, integrity and availability of their services. Users have no responsibilities about anything.

B. Platform as a Service Model

This model provides the user to deploy user-built applications onto the cloud infrastructure that are built using programming languages and software tools supported by the provider (e.g., Java, python, .Net). The user does not manage the underlying cloud infrastructure [3]. PaaS supplies all the resources required to build applications and services completely from the Internet, without having to download or install software. A downfall to PaaS is a lack of interoperability and portability among providers. That is, if you create an application with one cloud provider and decide to move to another provider, you may not be able to do so—or you'll have to pay a high price. Also, if the provider goes out of business, your applications and your data will be lost. Degree of control by providers is medium and they are only responsible for integrity and availability of their services. But users' responsibility is medium and they are responsible of confidentiality and data privacy. For example, users can use their data encryption and authentication systems in application level but security in other levels is in the provider's hands and they must be able to guarantee that the data remains secure from other applications.

C. Infrastructure as a Service Model

IaaS model lets the development organization define its own software environment [1]. Where SaaS and PaaS are providing applications to customers, IaaS doesn't. It simply offers the hardware so that your organization can put whatever they want onto it. This basically delivers virtual machine images to the IaaS provider, instead of programs, and the machines can contain whatever the developers want.

Degree of control by providers is low and they are only responsible for availability of their services. But users'

responsibility is high and they are responsible of confidentiality, data privacy and integrity. Fig. 1 shows provider and user responsibility in security of cloud service models.

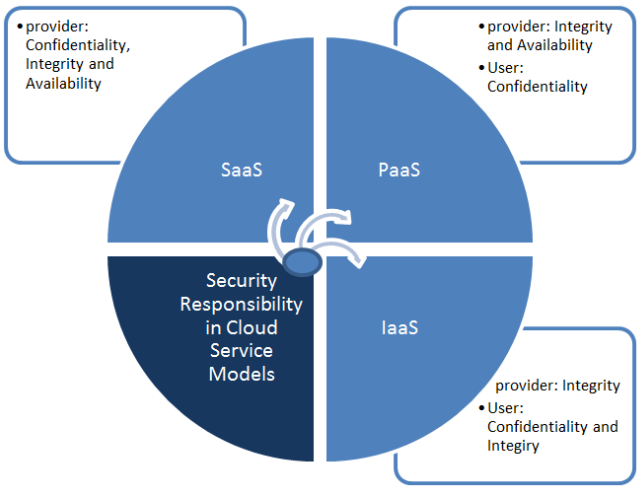

Fig. 1. Responsibility of users and providers in security of cloud service models

III. Data Security Model

In this section, in particular data security in cloud computing is examined. In today's world the most important security problem in the use of cloud computing at all levels is data security problem. In data security, confidentiality, integrity and availability of data in cloud computing are referred.

A. Data Confidentiality in Cloud

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. Data confidentiality is one of the most difficult things to guarantee in a cloud computing environment. In Cloud computing environment, two categories of confidentiality exists: confidentiality in private cloud and confidentiality in public cloud. Because the confidentiality in private cloud is like a simple private network, we go through the public ones. In public cloud there are some potential concerns about confidentiality. First, are there any access controls to protect the data? Access control consists of authentication and authorization. Todays the ways providers ensure that users are adequately authenticated when using browsers to access services in the cloud are limit. They must use strong ways in addition to username and password checking. Some new ways are 2 or 3 factor authentication or web proxy logon [6] and using Security Assertion Markup Language (SAML) standard. With SAML, each organization manages its own users and through trust relationships share authentication between sites. SAML is an elegant solution for scalable authentication. Authentication for the cloud will rely on SAML and provide the dual benefit of reducing the number of passwords that users must remember as well as improve user experience through Single Sign On (SSO). Second, are there any data encryption methods while data is transiting between end-user's client and the cloud's server? Data encryption is useful for kind of data that is stored on cloud servers and the users don't need to index or search them. About data-at-rest in IaaS encryption is a good idea, but encrypting data-at-rest in that a PaaS and SaaS cloud-based application is using as a compensating control is not feasible [7]. There are some works which allows data to be processed without being decrypted such as homomorphic encryption [8] and predicate encryption [9] that are underway.

B. Data Integrity in Cloud

Integrity is the assurance that the information is authentic and complete. The integrity of data is not only whether the data is correct, but whether it can be trusted and relied upon. Since 1980's we use "ACID" (atomicity, consistency, isolation, and durability) principles in our database management systems to ensure about data integrity but cloud computing is new enough that not all service providers have satisfactorily incorporated these data integrity principles in their solutions. Moreover, customers sometimes use such a variety of service providers that no single one of them takes responsibility for ensuring data integrity at the level of data entry and transaction management. There are some new standards that are related to cloud data management and over the time they are developing. Cloud Service providers must use and develop such standard to ensure their users about the integrity of cloud data. Internet is the media that are used in cloud computing and often the entry of it, is web applications. Some of the standards that are developing in today's cloud world are Data Integrity Field (DIF), SNIA Cloud Data Management Interface (CDMI), and XML-based solutions.

C. Data Availability in Cloud

Availability is the assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them. The most problematic issue in security of cloud computing is availability. Many of cloud service providers experienced downtime. There are some ways to provide data availability for customers for example some cloud service providers do back up customer data, or a better way is a caching proxy server that can reply to service requests without contacting the specified server, by retrieving content saved from a previous request, made by the same client or even other clients. Another way to have availability is switchover from the online-server to the hot-standby server. These range from storage mirroring across multiple servers which ensures that a server failure never results in data loss, to the ability to recover from a failure of the cloud controller, to high-availability features built into the catalog appliances. The ability to easily run two identical instances of the application on the same cloud, or in different data centers, provide the ultimate approach to high availability.

IV. Proposed Model

In this section, a new model for protecting data in cloud computing environments using the information stated in the previous section is offered.

Open Security Architecture (OSA) provides free frameworks that are easily integrated in applications, for the security architecture community. In [10], there are the

components of cloud computing architectures along with descriptions of elements that make it secure. In this paper, the model is enhanced to a new model for data security in cloud computing. In proposed model, all the techniques that are useful for protecting data in all levels of cloud environments from unsecure access are summarized. Different techniques for protecting different kind of cloud service providers are described in Fig. 2 in details. End users access the cloud environment via internet as an entry point that this entry must be secure. Strong log-in to access the cloud is advantageous for the cloud provider but disadvantageous for the users. This model must ensure security on the end users and on the cloud alike. The cloud needs to be secure from any user with malicious intent that may attempt to gain access to information or shut down a service. For this reason, the cloud should include a denial of service (DoS) protection. Using more bandwidth and better computational power is a good way which the cloud has abundantly.

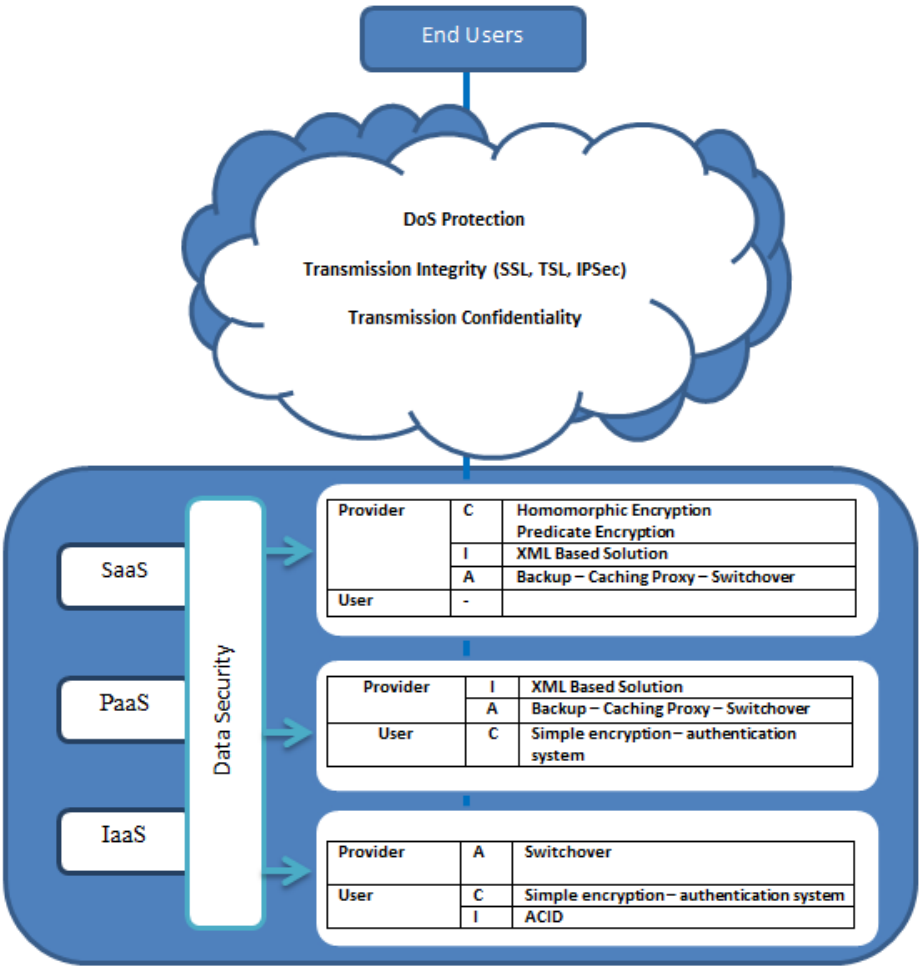

Fig. 2. A New Model for Data Security in Cloud Computing

After logging in to cloud, it must be pay attention to data transmission between users and the cloud provider. Encrypting data before sending them by users is a good way. For sending data, some transmission techniques like SSL, TSL and IPSec are good ideas. Another middle point between end users and the cloud that must be secure is that no one must be listening on the conversation between authenticated users and the cloud.

The same mechanisms mentioned above can also guarantee confidentiality. The cloud providers have the main responsibility for protecting data and each service providers use especial techniques for securing the resources. In this model according to previous section, it categorizes in three layers and in each layer it categorizes to main aspect of security that is confidentiality, integrity and availability.

V. Conclusion

As computing takes a step forward to cloud computing, we must pay attention to security issues of it. Because of security concerns, cloud computing is not concerned with some users. As a virtual environment cloud computing has its special security threats and these threats are completely different from threats in physical systems. In this paper, security concerns about data security in cloud computing is examined and a new model suggested for this environments. In this model security concerns and their solutions are categorized in three layers of security services to secure accessing to data resources in cloud worlds.

Although you may be transferring some of the operational responsibilities to the provider, the level of responsibilities

will vary and will depend on a variety of factors, including the service delivery model (SPI), provider service-level agreement (SLA), and provider-specific capabilities to support the extension of your internal security management processes and tools. In this model, the relationship between end users and cloud service providers is showed and according to their responsibilities in providing data security in cloud environment, a new solution for it is proposed.

Because in information security, most foundations can be built upon confidentiality, integrity, and availability, and CIA is a widely used benchmark for evaluation of information systems security, this model can be a good idea in cloud world that is a new world. Well-established security management processes are also aligned with an organization's IT policies and standards, with the goal of protecting the confidentiality, integrity, and availability of information. The proposed model pays attention to CIA in all three layers of services that cloud providers offer to their users.

REFERENCES

[1] J. Viega and McAffee, "Cloud Computing and the Common Man," *Published by the IEEE Computer Society*. 2009.

[2] A. Costanzo, M. Assuncao, and R. Buyya, "Harnessing Cloud Technologies for a Virtualized Distributed Computing Infrastructure," *IEEE Internet Computing*, Sept. 2009.

[3] C. Hoffa, et al., "On the Use of Cloud Computing for Scientific Workflows," *IEEE Fourth Int'l Conf. oneScience*, Dec. 2008.

[4] I. Foster, Ian; Y. Zhao, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared," *Grid Computing Environments Workshop*, pp. 12-16, Nov. 2008.

[5] B. Sotomayor, et al, "Virtual Infrastructure Management in Private and Hybrid Clouds," *IEEE Internet Computing*, Sept. 2009.

[6] E. Talmor, "Strong Authentication for Cloud Computing," http://sentry-com.net/blog/?p=125.

[7] T. Mather, S. Kumaraswamy, and Sh. Latif, "Cloud Security and Privacy", *Published by O'Reilly Media*, September 2009.

[8] D. Boneh, E. J. Goh, and K. Nissim, "Evaluating 2-DNF Formulas on Ciphertexts," LNCS vol. 3378/2005, pp. 325-341, ©Springer Berlin Heidelberg, 2005.

[9] J. Katz, A. Sahai, and B. Waters, "Predicate Encryption, Supporting Disjunctions, Polynomial Equations, and Inner Products," LNCS vol. 4965/2008, pp. 146-162, ©Springer Berlin Heidelberg, 2008.

[10] T. Andrei, "Cloud Computing Challenges and Related Security Issues. A Survey Paper," *Open Security Architecture society*.

Sh. Ajoudanian received her BS in 2005 from Islamic Azad University, Najafabad Brach, and MS in 2008 from Islamic Azad university, Najafabad Brach. She is currently Ph.D. Candidate in Computer Engineering Department, Islamic Azad University Science and Research Branch, Tehran, Iran . She is faculty member in the department of ComputerEngineering of Islamic Azad university of Najafabad .