Journal of Advanced Computing Research Vol. 1, Issue 2 (2016) 3-6

A New Software Development for Security Purposes on Cloud Computing

Syahirah bt Abdul Rashid [#1], Mohamed Faidz Mohamed Said [#2]

[#] *Universiti Teknologi MARA*
70300 Seremban, Negeri Sembilan, MALAYSIA
[1] syahirahrashid7@gmail.com
[2] faidzms@ieee.org

***Abstract*—Cloud computing is gaining popularity and on-demand access among computer users. Due to this, security in cloud computing has gain attention and became an important element in cloud computing. In this paper, brief explanation on cloud computing and several security issues are discussed including traditional security challenges and cloud security challenges. Although there are many new technologies that can improve security technologies yet there is no one solution for all the problem which means standard solution does not exist.**

Keywords: **traditional security issues, cloud security challenges**

I. INTRODUCTION

According to [1], cloud computing is relatively new and emerging term which is used by many organizations. As cited by [2], many organizations that are related to cloud computing make a huge of enterprises and individual users outsource their data into the cloud server. According to [3], in cloud computing, distributed data sharing among the members is important to accomplish network wide goals. Based on [4], cloud computing is a promising next-generation computing paradigm which incorporates different existing and new advancements. Cloud computing can be classified according to their deployment or service model. According to [5-7], cloud deployment models consists of private cloud, public, community and hybrid cloud. Private cloud is the cloud resources devoted to only one organization and used only for their organization. For instance, a cloud is built by one organization is used to serve their business critical applications. Besides that, public cloud is owned by service provider but its cloud resources are sold to public use as a self-service, on-demand and pay per use. For instance, these service providers are Google and Amazon. Community cloud is shared by several organizations that share same interest. An example, a school may create a community cloud for region school access and usage but this school must agree to follow a policy of cloud computing. Hybrid cloud is combination of private, public and community cloud. For example, an organization using a public platform to send data to a private cloud. As cited by [5, 8, 9], cloud computing licenses users to use cloud services on the fly in pay-as-you-go manner through the Internet. The services might be Infrastructure as a service (IaaS), Data storage as a Service (DaaS), Communication as a Service (CaaS), Security as a Service (SecaaS), Hardware as a Service (HaaS), Software as a Service (SaaS), Business as a Service (BaaS), and Platform as a Service (PaaS). Based on [10], these models likewise put a distinctive level of security necessity in the cloud environment IaaS and the establishment of all cloud services, with PaaS based upon it and SaaS thus based upon it.

According to [11], as the cloud computing increases, security is the main obstacle for this new imagined vision of computing capability. Based on [12], increasing volume of individual and essential information, raises more concentrate on storing the information safely. Security issues are being voiced out since security is an important element in cloud computing. Effectiveness of traditional protection mechanisms are being reconsidered and these creates traditional security challenges and at the same time there are issues introduced by the cloud computing which is cloud security challenges.

A. Traditional Security Challenges

The use of cloud computing proposes new attack vectors which make it easier to attack the cloud computing. Moreover, the availability of cloud service providers creates many problems where if the cloud service is disturbed, it greatly affects more since the cloud has the higher number of customers than in traditional model. For instance, a disruption in Amazon cloud results in several websites down including Foursquare, Reddit and Quara. According to [1], multi-tenant environment may lead to many vulnerabilities, where virtual machines disturb all users in the same physical server. As stated by [13], multi-tenancy leads to high risks of data visibility to other users.

B. Cloud security challenges

Based on [14], cloud service providers access full control over the stored data in the cloud. They can perform malicious tasks such as copy, destroying and modifying. As the end-users eager to know where their information is stored, and who control the information of the data, privacy and user data confidentiality is in concerns. According to [1], customers want to be guaranteed that the information is not used illegally and cannot be accessed easily. Others security challenges in the cloud computing include, resource

location in which end-users use the service provided without knowing where the information are located and this could create problem when argument happen it is beyond the cloud provider control. Besides that, authentication and trust of information is needed where the data that have been stored in cloud provider infrastructure may be altered by owner consent and data authenticity is important to ensure data integrity do exist.

C. *Data privacy and integrity*

Based on [14], the number of cloud users is increasing exponentially because of simplicity of the cloud and applications hosted on the cloud is in very high range. Due to this, security threats are increasing towards cloud clients. Data entity will lead to data breach and takes an unauthorized access to all the data that belongs to users if the attackers successfully penetrate the cloud. Because of integrity violation, cloud data lost multi-tenants in nature. For example, Saas providers may lost the data and have high risk over data storage.

D. *Availability*

According to [11], property of system can be accessible and processed, although the system only allows authorized entity. However, the system can be carried out even when some authorities misbehave. The meaning of availability refers to data, software and hardware is being available upon demand. Cloud computing resources present heavy reliance on resource infrastructures and network availability at all times.

Documenting specific user requirement is imperative in designing a solution. The multiuser distributed environment proposes unique security technique.

Table 1 shows that the level in which the user operates, application, virtual or physical.

Table 1. User-specific security requirement.

Level	Service level	Users	Security requirements	Threats
Application level	Software as a Service (SaS)	End client applies to a person or organization who subscribes to a service offered by a cloud provider and is accountable for its use	• Privacy in multitenant environment • Data protection from exposure (remnants) • Access control • Communication protection • Software security • Service availability	• Interception • Modification of data at rest and in transit • Data interruption (deletion) • Privacy breach • Impersonation • Session hijacking • Traffic flow analysis • Exposure in network
Virtual level	Platform as a Service (PaS) Infrastructure as a Service (IaS)	Developer–moderator applies to a person or organization that deploys software on a cloud infrastructure	• Access control • Application security • Data security, (data in transit, data at rest, remanence) • Cloud management control security • Secure images • Virtual cloud protection • Communication security	• Programming flaws • Software modification • Software interruption (deletion) • Impersonation • Session hijacking • Traffic flow analysis • Exposure in network • Defacement • Connection flooding • DDOS • Impersonation • Disrupting communications
Physical level	Physical datacenter	Owner applies to a person or organization that owns the infrastructure upon which clouds are deployed	• Legal not abusive use of cloud computing • Hardware security • Hardware reliability • Network protection • Network resources protection	• Network attacks • Connection flooding • DDOS • Hardware interruption • Hardware theft • Hardware modification • Misuse of infrastructure • Natural disasters

II. CONTRACTUAL AND LEGAL ISSUES

A new service level agreement for cloud security has been introduced which is Service Level Agreements (SLAs) and trusted data sharing over untrusted cloud storage providers for the control of the security challengers.

A. *Service Level Agreements(SLAs)*

According to [14], SLA can be described as protocol and it specifies as an set of the conditions and terms among user and cloud service provider. User must be clear from the perspective of security of their resources and others requirement that must be agreed upon SLA. Based on [1], SLAs define minimum performance level in which the customer can forecast for example only 99.999% system availability for outsourcing computation and storage to an external provider. SLAs do not support confidentiality and integrity and its security services level based on how much a customer is willing to pay. Security SLAs lifecycle are as follow:

- User will be consulted to a particular SLA to which the provider will confer, and the service will be provisioned.
- User may want to monitor the service to guarantee that the consulted SLA is being followed by the provider.
- If the consulted SLA cannot perform the previously SLAs, this will be relegated to numerous levels.

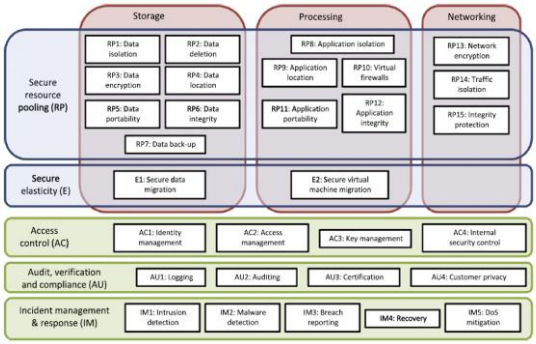

Figure 1. A framework for security mechanisms for SLAs

B. *Legal issues*

According to [13], legal issues in the cloud computing emerge because of CSP assets in geologically unique and conflicting legal jurisdictions. The chance that the information is relocated to various area having diverse laws, is troublesome for users to arrange the security strategies to concur with new legal jurisdictions. Once in a while, the information may exhibit in more than one area having diverse laws about digital security.

III. TRUSTED DATA SHARING OVER UNTRUSTED CLOUD STORAGE PROVIDERS

Based on [1], owners have just constrained control over the cloud computing, accordingly they should set up component to order the authorization of security policies to guarantee data confidentiality and integrity. A low trust level when clients sharing information to the cloud in view of cloud services providers has over many benefits by

permitting them to broad control and capacity to adjust client IT framework. Due to this, secure system is needed to enable trusted data sharing through untrusted cloud providers. Below are several security requirements in cloud computing for data storage as displayed by Figure 2.

- The data should be kept private when storing on the cloud so that the cloud storage provider could not compromise the data confidentiality by any means.
- Owners of the data has full control over authorization of data sharing. With the permission from the owners, the designated user can then access the data kept on the cloud.
- Only an intended user should be given data access authorization.

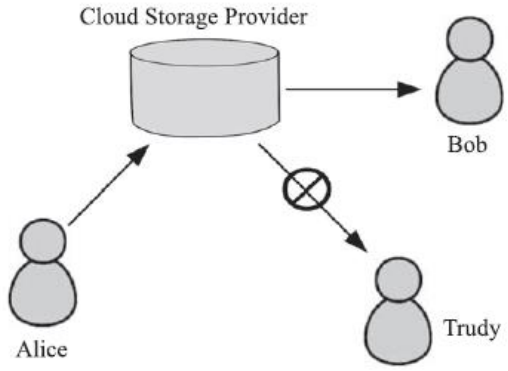

Figure 2 : Secure sharing on cloud

The requirement to secure the data storing could be achieved by either homomorphic encryption or incremental encryption.

i. Homomorphic encryption

Algebraic operations connected on ciphertext are reflected in the comparing plaintext. Third party can compute sum of two encrypted numbers. When the message is returned to client, it can be encrypted by utilizing unique key and the outcome is the same as aggregate of the two numbers plaintext. By doing this, different gatherings can produce a ciphertext without knowing plaintext others deal with.

ii. Incremental encryption

The procedure permits users to have trusted information data storage to sharing over untrusted cloud storage provider. This allows the users to deal with their own particular information on any cloud storage provider. The general thought is to encrypt the information before storing in the cloud. The encrypted information is being re-encrypted without decrypt the information first. The re-encrypted information is just to the approved client utilizing cryptographically available.

The cryptographically accessible process does no reveal the clear text data to the cloud provider at any time. The data is encrypted with different keys at different stages. The data is in encrypted form all the time until it is sent to authorized access. This ensures the data does not disclose the information to any parties. Figure 3 illustrates data leakage prevention.

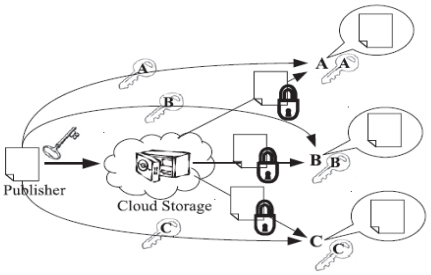

Figure 3 : A cloud data leakage prevention solution.

IV. LITERATURE SOLUTION

In this section, the solution for the security challenges that being faced are discussed.

A. Data storage issues solutions

The SecCloud provides a storage security protocol to secure the data stored on the cloud. According to [14], SecCloud protocol stores the data in secure mode using encryption. Multiplicative groups and cyclic additive pairing are used for key generation for cloud consumers CSP and others. The encrypted data along with the verifiable signature is sent to cloud data center together with session key. The session key is generated using Diffie-Hellman algorithm for both bilinear groups. The cloud decrypts the data, verifies the digital signature and store the data in the specific location in the cloud. The SecCloud then verify whether the data is stored at specified location or not. For computation security in SecCloud protocol, the Markle hash tree is used. The verifying agencies will verify the computational result using Markle hash tree.

B. Data privacy and integrity solutions

The File Assured Deletion (FADE) protocol gives a key management with data integrity and privacy. Based on [14], it is a light weight protocol and uses both asymmetric and symmetric key encryption in key management because FADE is simple. Symmetric and asymmetric keys are protected by Shamir scheme to generate the trust in the key management. FADE protocol uses group of key managers, those who acts as a trusted third party. The client used key k as an encryption key for file F and the other key used for encryption data key (k). User must request the key pair from the third-party policy to upload the data to the cloud. Users receive public and private key from key manager and the uploaded file encrypts randomly generated k and k is encrypted with symmetric key. MAC is generated for integrity check and encrypted file is decrypted with the public key of key pair. The reverse process is done by the receiver to transform back the messages into original.

C. Public Key Infrastructure

Public key infrastructure is technically sound and legally acceptable to implement strong authentication, authorization, data confidentiality, data integrity and non-repudiation. PKI benefits from the coupling with a directory. Directory is a set of objects with same attributes organized in a logical and hierarchical manner. A Trusted Third Party assuring specific security characteristics within cloud environment. Combination of Public Key Cryptography, Single-Sign-On technology and LDAP directories to securely identifies and authenticate implicated entities. Based on [11], Public Key Infrastructure is be able to transform security problems into key management issues. Unfortunately, the success of the proposed solution as in any cryptographic system depends on controlling access of private key.

V. METHODOLOGY

In order to solve traditional security challenges and cloud security challenges, there are many methods that have been used but in this paper the methods that have been discussed are trusted data sharing over untrusted data sharing, data storage issues solutions, data privacy and integrity solutions and public key infrastructure. In trusted data sharing over untrusted data sharing, the data that have been shared on the cloud must be keep private so that the cloud storage provider could not access it unnecessarily without the owner permission. In data storage issues solutions, SecCloud provide a security protocol to secure the data is stored on the cloud. The Diffie-Hellman algorithm is used to generate session key and verify the computational result by using Markle Hash Tree. Besides that, to find the solutions in data privacy and integrity solutions the File Assured Deletion (FADE) protocol have been used to provide key management with data integrity and privacy. The symmetric and asymmetric in key management are used because FADE is simple. Other than that, public key infrastructure provides legally acceptance to implement strong authentication, authorization, data confidentially, data integrity and non-repudiation. PKI can transform security problem into key management issues depending on controlling access of private key [15-17].

VI. CONCLUSION

Cloud computing is gaining popularity and on-demand access among computer users. Since this kind of computing is relatively new, many new technologies are essentially required to improve the security of this technologies. Yet there is no one solution for all the problems which means standard solution does not exist. This is because different security problem deals with different security solution. In further research, it is recommended that the method to find security solutions could be improved and be obtained in a short period of time.

REFERENCES

[1] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Computers & Electrical Engineering*, vol. 39, pp. 47-54, 2013.

[2] M. Miao, J. Wang, H. Li, and X. Chen, "Secure multi-server-aided data deduplication in cloud computing," *Pervasive and Mobile Computing*, vol. 24, pp. 129-137, 2015.

[3] Y. Lu and M. Zhu, "Secure cloud computing algorithms for discrete constrained potential games," *IFAC-PapersOnLine*, vol. 48, pp. 180-185, 2015.

[4] J. Li, X. Chen, Q. Huang, and D. S. Wong, "Digital provenance: Enabling secure data forensics in cloud computing," *Future Generation Computer Systems*, vol. 37, pp. 259-266, 2014.

[5] "<developing a scheduler Floyd-Warshall Algorithm.pdf>."

[6] D. C. Chou, "Cloud computing: A value creation model," *Computer Standards & Interfaces*, vol. 38, pp. 72-77, 2015.

[7] V. Mauch, M. Kunze, and M. Hillenbrand, "High performance cloud computing," *Future Generation Computer Systems*, vol. 29, pp. 1408-1416, 2013.

[8] A. N. Khan, M. L. Mat Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," *Future Generation Computer Systems*, vol. 29, pp. 1278-1299, 2013.

[9] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200-222, 2016.

[10] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, pp. 1-11, 2011.

[11] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, pp. 583-592, 2012.

[12] L. a. Tawalbeh, N. S. Darwazeh, R. S. Al-Qassas, and F. AlDosari, "A Secure Cloud Computing Model based on Data Classification," *Procedia Computer Science*, vol. 52, pp. 1153-1158, 2015.

[13] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357-383, 2015.

[14] N. vurukonda and B. T. Rao, "A Study on Data Storage Security Issues in Cloud Computing," *Procedia Computer Science*, vol. 92, pp. 128-135, 2016.

[15] M. F. M. Said, M. N. Taib, and S. Yahya, "Analysis of the CPU Utilization for Point-to-Point Communication Operations in a Beowulf Cluster System," in 2008 International Symposium on Information Technology, 2008, pp. 1-6.

[16] M. F. M. Said, M. N. Taib, and S. Yahya, "Analysis of TCP/IP Overhead on Overlapping Message Transfer and Computation in a Distributed Memory System Architecture," International Journal of Advanced Research in Computer Science (IJARCS), vol. 3, pp. 22-36, 2012.

[17] M. F. M. Said, S. Yahya, and M. N. Taib, "Analysis of Different Programming Primitives used in a Beowulf Cluster," International Journal of Computer and Information Technology (IJCIT), vol. 1, pp. 25-33, 2012.