An investigation in cloud computing security: problems and challenges

Mohammadjavad Hosseinpoor[1*], Mortaza zolfpour- Arokhlo[2]

Abstract— Cloud computing is a model in order to provide easy access to a common source in term of demands from adjustable computing sources (networks, servers, storing, applications and services) which Is capable of being provided quickly and deployed with the leas managerial efforts or interaction with service provider. In this regard, one of the main problems is security. In this research various security challenges in cloud computing was investigated in three sections and their importance is evaluated from least to most important.

Index Terms— Cloud computing, Cloud security, Challenges.

1 INTRODUCTION

Cloud computing is a model in order to provide easy access to a common source in term of demands from adjustable computing sources (networks, servers, storing, applications and services) which Is capable of being provided quickly and deployed with the leas managerial efforts or interaction with service provider. In fact, cloud computing is a new type of computation which provides uniform access to distributed sources in an extended area in term of demands [1, 2]. Their emergence affected increasingly the IT technology in recent decades and great companies such as Google, Amazon and Microsoft are seeking providing stronger, more reliable and economic platforms and there are many commercial companies are searching reshaping their commercial models[3,4]. So they can benefit from the advantage of cloud computing. Nevertheless, there are many problems with contemporary cloud computing. A new evaluation performed by cloud security association (CSA) indicates that the security became one of the main concerns of cloud computing users. Here are 5 key characteristics of cloud computing defined by NIST:

- Self-serving in term of demand: the client would be able to provide unidirectional computation capabilities unidirectional such as server time or network storage without need for human interaction or any other interactions with service providers
- Accessing the network everywhere: via standard mechanisms in heterogeneous thin and thick clients, it would be possible to access it and it is wideband and low delay.

- Accessing the network everywhere: via standard mechanisms in heterogeneous thin and thick clients, it would be possible to access it and it is wideband and low delay.

- Integration of time independent source: provider's computing sources are integrated so that they provide all customers with multi-client services and there are physical and virtual sources allocated dynamically based on customer's demand and then they would be allocated to next client.
- Quick flexibility: we allowed high or low scalability of sources, rapidly.
- Measured services: they are in major extracted from commercial model characteristics and indicate that cloud computing service provider controls and optimize the computational sources using automatic source allocation, balancing the cloud and measurement tools.

Software as a service (SaaS): In SaaS the commercial cloud computing software is provided for customers/clients as services in term of demand. Since clients receive software components from different providers and make use of them, the main issue would be that the managed information would be preserved by these combined services.

Platform as a service (PaaS): PaaS provides a program or development platform by which the user can run his program which is running in cloud.

Infrastructure as a service (IaaS): IaaS plays the role of a service like delivering computer hardware such as servers, networking technologies, storing and data center space. This model includes delivering OSs and source management virtualization technologies [5, 6, 7, and 8].

The cloud arrangement models as 4 as followings:

General cloud: in general cloud the sources are provided dynamically and in self-served manner using accurate adjustment on internet via web applications or services. Customers can access these sources rapidly and pay only for operational sources. Since several customers are making use of the sources jointly, so the main dangers in general cloud include security, following the bylaws and agreements and QoS.

Private cloud: in private cloud, computational sources are made use and controlled by a private company. In this cloud, the source accessibility is limited to customers who are belonging to the cloud owner organization. The main advantage of this model is that data security and privacy in enhanced, since obeying the regulations and QoS are under the control of the company.

Mixed cloud: the third type of cloud is a bigeneric one composed of private and general clouds. Through this inter-

- *[1]PhD student and member of faculty in Department of Computer Engineering and Member of Young researchers and elite club, Estahban Branch , Islamic Azad University, Estahban,Iran. Email: Mj.Hosseinpoor@outlook.com
- [2]Member of faculty in Department of Computer Engineering, Islamic Azad University Sepidan Branch, Sepidan, Iran
E-mail: Zolfpour@gmail.com

face an organization is able to provide certain services in a company and provide other services via other external companies.

Group cloud: cloud infrastructures are shared among some of the companies with mutual interests and similar demands. This can lead to limiting the investment costs of setting up the cloud, since the costs are shared among organizations. Cloud infrastructures can be hosted by a third party or located in community organizations] 9, 10, 11].

2 Cloud security Challenges

Organizations use cloud computing in many serving models such as (SaaS. IaaS and PaaS) and developed models such as (general, private and combinational). There are security issues and concerns related to cloud computing, but all are classified into 2 groups: first, security issues related to service providers and second, customers related security issues. Often, the provider has to make sure of the security of his/her infrastructure and protect the customers' data and applications; whereas, the customer has to make sure about the performance of service provider in line with creation of suitable security criteria in order to protect his/her data. The vast application of virtualization in implementing cloud computing has created similar security concerns for customers and general services of cloud computing. Virtualization is a good alternative link between OS and hardware in computation, storage and even network. This has led to a new layer known as virtual layer which itself needs management, adjustment and consistent security. The main concern with this regard is "hypervisors" or virtual software's compatibility. However, these concerns are mostly discussed theoretically; they can exist in real world. For example, an intrusion into management workstation which is making use of virtual management software can lead to breakdown of a database or its readjustment desirably for attackers [7, 12, 13, and 14].

3 Security challenges of SaaS

The computational interface is a multiple interface in which every area can make use of different security, privacy and reliability needs and potentially make use of different mechanisms, mediators and meanings. Main security challenges in SaaS and its related solutions are explained in next sections [7, 15, 16, and 17].

Identity authentication and management

Using cloud services, user is able to access information from different locations in internet. Therefore, we need for identity authentication mechanism to authenticate users' identity and providing them with services based on characteristics and licenses in hand. An IDM system has to be capable that protect private information and prevent from sensitive information related to users and processes from being unauthentic accessed. Each company has its IDM system in order to control the accessibility to information and computational sources.

Confidentiality management

In cloud computing interfaces, customer depends on service provider for various services. In most of the services, customer has to store the privacy data in provider's side. Therefore, reliability framework has to be developed so that it is allowed to capture sets of main parameters needed for reliability and management of reliability and interactional demands and sharing.

Accountancy and accessibility control

Due to heterogeneity of and diversity of computer services, an accurate accessibility has to be implemented. Access control service has to be flexible enough so that they meet needs based on dynamic access needs and characteristics based licenses. Access control model should have SLS related aspects. Since cloud computing model is a pay-for-usage model, therefore accountancy for creation of users' bills is necessary. In cloud, providers usually don't know the users and this is difficult to allocate the roles directly to users. Therefore, characteristics or credibility based policies can be applied for improving this capability. Security authentication marking language (SAML), expanded access control marking language (XACML) and webpage standards can be applied for determination of access control policies. Amongst proposed methods so far, role based access (RBAC) is widely accepted due to its simplicity, flexibility in dynamic needs perception and supporting for least score principle and effective score management.

Authenticated access

Authenticated access is an important information security in cloud computing which has to be considered for reliability on reference comprehensiveness. This section follows the application of control and considering the rights on process flow in cloud computing. In case of general cloud, several customers are shared which are in computing sources which are provided by a single provider. Data security needs preserving issues such as standardization, approaches of regulation and bylaws for preventing from unauthentic access, disclosure, copying, making use of or modifying the detectable personal information.

Comprehensiveness

Comprehensiveness refers to making use of necessary actions in cloud area while accessing data. Therefore, characteristics of ACID (Autonomy, compatibility, isolation and durability) of intra-cloud data undoubtedly have to exist in all models of cloud computing deliveries.

Reliability

In cloud computing, reliability plays a key role in controlling the organizational data which are located in multiple distributed databases. Creation of reliability of users' profiles and preserving their data while accessing, need informational security protocols which are implemented in different layers of applications. Reliability is one of the most difficult issues which can be guaranteed in general cloud computing interface. There are many reasons for this. First, as general cloud grows, so number of cloud providers' worker and customers' data accessibility (whether authentic or not) also increases and then reliability oppression potential sources increase. Second, the need for flexibility and error tolerance leads to mass copies and needs for caching many of data and this in turn can increase the possibility of data loss. Third, end-to-end data encryption is not available, yet. Therefore, data reliability would be increased using many of private clouds which are managed by reliable parties.

Accessibility

Accessibility is one of the most important issues in cloud computing information security since it is a key decision factor in decision making among private, general and combinational cloud sellers in analysis model. Service-level agreement is the most important document focusing on cloud services access and sources between providers and costumers. The goal of accessing the cloud computing systems (such as applications and its infrastructures) is to make sure about the fact that users are capable to make use of them whenever and wherever they desire. Many of cloud computing system vendors provide cloud infrastructures and platforms based on virtual machines. Therefore, accessibility is a compulsory security necessity for IaaS, PaaS in general and private clouds. All of services in private cloud are in company and then the access control is necessary when making use of SaaS.

4 Security challenges in PaaS

Service level agreement

SLA is a part of service agreement between customer and provider which is officially determining the level of services. This agreement is applied for identification and definition of customers' needs, reduction of paradox areas such as delivered services, tracking and reporting the regulatory obedience and dispute resolutions, customers' tasks and liabilities, security IRP and end of privacy information [7, 18, 19, and 20].

Non-denying

Non-denying in cloud computing scan be created using common E-trading security protocols and providing signs of transference of data in cloud applications such as digital signatures, time seals and receive verification services (digital receive verification of sent or received messages). User's data has to be preserved which includes:

1. Personal detectable information: this information includes every type of information which can be used for detecting or discovering an individual such as name, ID card number, address etc. second, data including the information which is related to other information for detection or positioning the person such as social relations information, postal code, internet IP address and credit card number.
2. Sensitive information: this information needs additional preserving actions. Naturally, this information includes race or religion, health, sexual orientation, membership in a union or other information or they are considered private. Some of researchers believe that other information can be considered as sensitive information. They think this information includes personal financial information, job performance information and other information which are detectable sensitive ones. They are including biometric or picture sets of cameras in public places.
3. Making use of data: this section includes information collected by computer devices such as printers and input devices. Also, they include behavioral information such as observing digital content habits, new visited websites and history of product consumption, social interaction or frequent places.
4. Individual-specific devices' identity: other types of information which may be tractable for a user's device such as IP addresses, Radio Frequency Identity labels are also single hardware information.

Declaration, openness and transparency

Cloud services provider has to explicitly explain that that the user of the cloud stored data is. For example, for what application they need data and how they make use of the, and how much of it would be maintained and whom they will share with and other data usages. If they wanted to change data usage, they have to inform and warn the users. If third party is given the information, they have to inform users. Personal information has to be collected directly from the users unless it is difficult task or for any reasons it would be impossible. Data security policies have to accessible via network or other forms of communication for users and their usage and understand has to be easy.

Right, permission and power

Cloud computing provider has to reserve the users' right to state whether they can collect the users' data or not. Collection, usage and personal detectable information disclosure permission has to be given by customer. But cloud computing provider has to have the power of control.

Minimization

Data which to be managed in permitted extension has to be collected in form of a set and used as shared set or disclosed. Access information and usage perspective also has to be minimized, simultaneously.

Accuracy

Data owners have to access the personal information so that they see what is going on and who is making use of them and be able to control data accurately. Necessary actions have to be performed in order to make sure that personal information is accurate and there is no need to modify them.

Limiting disclosure, usage and maintenance

Data has to be disclosed or used only for the purposes they are collected and only authentic parties who are permitted to make them used are given the data. Personal data has to be anonymous and integrated as much as possible to limit the documents conformity potential as much as possible. Personal information has to be maintained as long as they are needed.

Responsibility

Services providers in cloud have to provide arrangements to make sure about the policies of data security. Also, it is a reasonable and rational action to have an inspecting unit to supervise the accessibilities and data modification. This is related to responsibility.

5 Security challenges in IaaS

Data center security and preservation

In cloud computing, several customers can share, store and access data in cloud. Therefore, customer's data has to be differentiated in access by another one and one has to be able to transmit data securely from a location to another. Cloud services provider performs suitable security actions in order to prevent from data leakage or access by unauthentic third parties. The provider has to be careful to allocate scores to the customers and make sure that the allocation task cannot be changes even by the high rank users in cloud provider. Access control policies have to be performed accurately and properly.

When there is someone willing to access data, the system has to check the policy making regulations and data would be disclosed if these policies are met [21-25].

Privacy preservation

Data privacy preservation can create an anonymous data search engine to search data bilaterally and obtain needed data. Searchable contents are not detectable for the other party simultaneously and it is not possible to obtain an unrelated content during search process. Data privacy preserving is important in cloud computing in all life cycle phases of data.

Data transmission security

When someone is using a general cloud the most important risk in data transmission is not to make use of encryption algorithms. Company's data are moving throughout the network so that cloud computing provider processes them. How can we make sure that these data are not lost or stolen in process of data transmission in network? Also, how it is possible to make sure that cloud computing provider maintain data in privacy in company and there would not be any data leakage in cloud computing side? Id data transmission is encrypted, then due to the problems in data processing it is possible to lead not being indexed or lack of data searched [7, 12, 26, and 27].

Data migration security

In cloud computing, data exists in networks and every network has several backups. Data security is the main focus of this research. The national military secrets are not generally disclosed. If a military unit considered making use of cloud computing, it has to make sure that data are secured in cloud. Since the cloud interface is a DNI Amazon EC2 interface, so data migration security has to be considered. This is one of the hot discussions about cloud computing.

Data residues

Data residue means that the remained data are deleted after physical performance and storing interface also delete the records which can rebuild data physical characteristics. In cloud computing interface, the remained data possibility discloses the sensitive information unintentionally; therefore, cloud services providers has to be able to detect and identify the user cloud by cloud to make sure that before this space is allocated to other users, the storage space would be cleared where data are shared. These residues have to be deleted from every space for storing such as disk or memory. Cloud providers have to delete the system files, directories and sources such as database records completely before they allocate the cloud interface to other users.

Data listening during passage

Cloud computing is a distributed architecture and points to more data passing than traditional infrastructures. For example, data has to be transmitted between some physical machines, cloud infrastructure and web service receivers remotely etc. in order to synchronize the images of some distributed machines.

Data unsecure and ineffective deletion

When a provider is changed, sources decrease gradually, the physical hardware is reallocated etc. so, data may exist in a certain lifecycle in security policy. This can be impossible to perform certain processes in security policy, since complete data deletion is possible only by destroying the disk on which data of other service receivers is stored. When there is a decision made on deletion of a cloud source, this is not resulted in complete data omission [28].

Cloud service engine security

Each cloud architectures depends on a particular policy which service engine is located on physical hardware sources and manage the customer's sources in different levels of abstraction. Service engine is developed and supported based on the vendors' policies and open source community in various cases. This can be customized by more cloud computing providers from security viewpoint [8, 15, and 28].

6 Conclusion

This article investigated many of challenges in cloud computing systems and cloud operations faced. Security issues and challenges are classified into 3 groups based on their function and permeability: 1) security challenges in Software as a service (SaaS), 2) security challenges in platform as a service (PaaS) and, 3) security challenges in infrastructure as a service (IaaS); which are investigated based on table 1 from importance level perspective. As it is observed, many of the challenges are of significant importance to consider them particularly is a very important issue in cloud computing structure. Therefore, other challenges are to be considered based the importance level of these cases.

TABLE 1
Investigation into Security Challenges in Cloud Computing from Type and Importance Level Perspective

Challenge	Security challenge	Importance level
Security challenges in SaaS	Identity authentication and management	high
	Confidentiality management	Medium
	Accountancy and accessibility control	High
	Authenticated access	Very high
	Comprehensiveness	Very high
	Reliability	High
	Service level agreement	Very high
	Accessibility	Medium
Security challenges in PaaS	Service level agreement	Very high
	Non-denying	Medium
	Declaration, openness and transparency	Very high
	Right, permission and power	High
	Minimization	low
	Accuracy	High

	Limiting disclosure, usage and maintenance	Medium
	Responsibility	high
Security challenges in IaaS	Data center security and preservation	Very high
	Data listening during passage	High
	Data residues	Medium
	Data migration security	High
	Data transmission security	High
	Privacy preservation	Very high
	Cloud service engine security	High
	Data unsecure and ineffective deletion	Medium

REFERENCES

[1] Mj. Hosseinpoor, H. Monem, M. Zolfpour- Arokhlo, “Presenting an Optimum Method in Running Global Query on Distributed Database System” , International Journal of Advanced Research in Computer Science and Electronics Engineering,Vol 4., No 4.,2015

[2] M.Marwaha, R.Bedi, “Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing",International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, 2013.

[3] Mj. Hosseinpoor., H. Kazemi., “Present a New Middleware to Control and Management Database Distributed Environment”, International Journal of Emerging Technology and Advanced Engineering, Vol 3, Issue 5, 2013.

[4] G. Kulkarni,J.Gambhir, T. Patil, A. Dongare, “A Security Aspects in Cloud Computing”, IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS), 2012.

[5] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom., ” Cloud Computing Security: From Single to Multi-Clouds”, 45th Hawaii International Conference on System Sciences, 2012.

[6] W.Liu, “Research on Cloud Computing Security Problem and Strategy”, 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012.

[7] A. Bouayad, A.Blilat, N.H. MEJHED, M.E.GHAZI.,” Cloud computing : security challenges”, Colloquium in Information Science and Technology (CIST), 2012.

[8] I.M. Khalil, A. Khreishah, S. Bouktif, A. Ahmad., “Security Concerns in Cloud Computing”, 10th International Conference on Information Technology: New Generations, 2013.

[9] H. Yu., N. Powell., D.Stembridge., X. Yuan., “ Cloud Computing and security challenges”, ACM-SE '12 Proceedings of the 50th Annual Southeast Regional Conference, 2012.

[10] M.K. Srinivasan, K. Sarukesi, P. Rodrigues, S.Manoj M, P. Revathy, “State-of-the-art Cloud Computing Security Taxonomies – A classification of security challenges in the present cloud computing environment”, In proceeding of: ACM International Conference on Advances in Computing, Communications and Informatics, ICACCI 2012, Volume: ISBN: 0978-1-4503-1196-0.

[11] V.KRISHNA REDDY 1, Dr. L.S.S.REDDY., "Security Architecture of Cloud Computing", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 9 September 2011.

[12] Danish Jamil Hassan Zaki., "Cloud Computing Security", International lournal of Engineering Science and Technology (IJEST), Vol. 3 No. 4, 2011

[13] Michael Gregg.”Security Concerns for CloudComputing”, Technical Report. Global Knowledge,2010.

[14] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy. March 2012. SLAs in Cloud Systems: The Business Perspective. International Journal of Computer Science and Technology. Vol. 3, Issue 1. Page no. 481-488.

[15] Jansen, W.A.. Cloud Hooks: Security and Privacy Issues in Cloud Computing. Proceedings of 44th Hawaii International Conference on System Sciences.PageNo.1-10, 2011.

[16] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data storage security in cloud computing", ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, 2010, pp. 1-9.

[17] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6), 2010, pp. 24-31.

[18] E. Mathisen, “Security challenges and solutions in cloud computing,” in 2011 Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies Conference (DEST), 2011, pp. 208–212.

[19] S. Thalmann, D. Bachlechner, L. Demetz, and R. Maier, “Challenges in Cross-Organizational Security Management,” in 2012 45th Hawaii International Conference on System Science (HICSS), 2012, pp.5480–5489.

[20] F.Sabahi, “Virtualization-level security in cloud computing,” in 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), 2011, pp. 250–254.

[21] C. Wang, Q. Wang, K. Ren, and W. Lou, “Towards Secure and Dependable Storage Services in Cloud Computing,” IEEE Transactions on Services Computing, vol. PP, no. 99, pp. 1–1.

[22] Lingfeng Chen and D. B. Hoang, “Towards Scalable, Fine-Grained, Intrusion-Tolerant Data Protection Models for Healthcare Cloud,” in 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011, pp. 126–133.

[23] Haoyong Lv and Yin Hu, “Analysis and Research about CloudComputing Security Protect Policy,” in 2011 International Conference on Intelligence Science and Information Engineering (ISIE), 2011, pp. 214–216.

[24] O. Popovic, Z. Jovanovic, N. Jovanovic, and R. Popovic, “A comparison and security analysis of the cloud computing software platforms,” in 2011 10th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS), 2011, vol. 2, pp. 632–634.

[25] I.Gul, A. ur Rehman, and M. H. Islam, “Cloud computing security auditing,” in 2011 The 2nd International Conference on Next Generation Information Technology (ICNIT), 2011, pp. 143–148.

[26] A.Tripathi and A. Mishra, “Cloud computing security considerations,” in 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), 2011, pp. 1–5.

[27] S. Sengupta, V. Kaulgud, and V. S. Sharma, “Cloud Computing Security--Trends and Research Directions,” in 2011 IEEE World Congress on Services (SERVICES), 2011, pp. 524–531.

[28] J. Wu, L. Ping, X. Ge, Y. Wang and J. Fu, “Cloud Storage s the Infra-

structure of Cloud Computing", IEEE Int. Conf. on Intelligent Computing and Cognitive Informatics, June 2010.