International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-3, Issue-5, May 2017
ISSN: 2395-3470
www.ijseas.com

A Comparative on Cloud Computing Security Mechanisms

Mohammadjavad Hosseinpoor[*1], Fatemehsoghra Zolfi[2], Rayhaneh Mosalanezhad[3]
[1*] Member of faculty in Department of Computer Engineering and Member of Young researchers and elite club, Estahban Branch, Islamic Azad University, Estahban,Iran
[2,3] Department of Computer Engineering and Member of Young researchers and elite club, Estahban Branch, Islamic Azad University, Estahban

Abstract
Today's with the increasing spread of computers and the human dependency to the digital world, Researchers are always looking for ways to speed up and improve services provided for customers and cloud computing enables us to achieve this. Cloud computing that provides the on-demand model and automatic service features, satisfies Company executive's needs and customer's requests with an incredible cost and easy management practice in three levels of SaaS, PaaS, IaaS. So, Improve the security of cloud computing is important for a wide use in a real application. In this paper, we studied the security of web applications and application programming interfaces [API].
Keywords: *Cloud computing, web applications, security, API.*

1. Introduction

Today's with the increasing spread of computers and the human dependency to the digital world, Researchers are always looking for ways to speed up and improve services provided for customers and cloud computing enables us to achieve this. Cloud computing is an emerging area in computer science and it is so called because of the data and applications of Web servers located in the cloud. Simply, cloud computing means sharing of programs and resources in a network environment, without importance of the ownership and management of network resources and applications. Currently, there is no standard definition of cloud computing, however, the definition that most scholars agree it is as follows:
Cloud computing is a model for easy access to a collection of computing resources, these resources [eg, networks, servers, storage, applications and services] are subject to change and configure. In cloud computing, resource management, and supplier's direct intervention can be minimized and services are provided or released quickly. An issue that has recently been considered in cloud computing, is "security", however, security is still a major challenge in cloud computing. In the other hand, in order to establish and maintain security we should pay attention to review and determine the possible threats and to protect the security process.
Cloud computing provides a virtual resource for customers. Cloud services are available to the customer via the Internet [8]. Web applications are used to access and manage cloud resources which have led to these programs to become one of the important components of cloud computing [18]. Customer's processes are done in virtual environments that use the physical resources as result [9]. Multiple processes of different virtual users are assigned to the same physical machines that these machines are logically isolated. This creates a multi-property environment in the cloud. Despite its advantages, cloud computing is not without security risks that these risks are very critical [2]. One of the most effective security solutions in cloud computing is "virtualization". Virtualization can be used as one of security components. Many organizations use cloud computing in service models such as [Software as a Service, Infrastructure as a Service and Platform as a Service] and developed models such as [private, public and hybrid] are used. Issues and security concerns associated with cloud computing is that in this article, these challenges are examined in two general categories:
First, security issues related to identity management and access control. And second, security issues related to the security of web applications and application programming interface. The solutions available to improve security at these two levels is studied.

2. Identity Management and Access Control

Subheadings in a cloud environment, confidentiality and integrity of data and services are also related to identity management and access control. Following user authentication and control unauthorized access to information is a very important issue [12]. The issue of identity management and access control in a cloud environment becomes more complex because resources and their owners are in different administrative areas and in its current form, may not carry the authority and authenticity to the cloud environment [3]. In addition, unlike traditional IT, cloud may be facing members of different organizations and with different identities and authority that are using the same physical resources at the same time [12]. Use powers and authentication systems separately for internal organization and cloud, may create complex conditions over time [13]. Cloud services are elastic and dynamic, IP addresses are regularly replaced, and the service began to work in a shorter time. The property of "pay as used" allow users to continuously join and leave cloud. All these features make traditional access control systems and identity management not sufficient for cloud environments [4]. A dynamic cloud mechanism needs a suitable composition and strict access control to be able to control the unauthorized activity within the cloud [10]. In addition, here we need organizations to control identity management system so at the time of joining and leaving staff update quickly access control policies [28]. As a result of weaknesses in identity management and access control, many problems can be created in the cloud. For example, lack of access to services due account locking, weak mechanisms to reset credentials, inadequate inspection and control permissions, authentication between areas, inadequate monitoring and chronology, weakness in XACML messages, and XML attacks.

3.Web application security and application programming interface [API]

Services and programs is offered to users by Internet [16]. In fact, using and management on the Web, is one of the essential requirements of cloud applications [127]. The program is provided by cloud service providers, are always on the cloud and cloud users everywhere have access to it. One of the most important characteristics of cloud software is that they are not restricted to specific users [28]. Different users may have access to similar programs that may be at the same time. Vulnerabilities of cloud applications is similar to traditional web applications and technology. Since the vulnerability of applications in the cloud is much more destructive than traditional, web applications traditional security solutions for cloud computing environment is not enough. Multiple users, their data, and other resources being at the same place make it a bigger problem. 10 The main risks in Web applications is identified by "free web application security project" in 2013 include:

- penetration [SQL OS and LDAP]
- authentication step getting inefficient
- Cross-site scripting [Site-Cross] [XSS]
- insecure direct object references
- Security configuration error
- disclosure of sensitive data
- Losing control, the level of access
- Cross-site forgery requests [CSRF]
- Use of known vulnerable components
- redirect and invalid forward

To protect Web applications and user's resources in development, deployment and management of Web applications, the above-mentioned risks should be considered. In cloud, users have access to services by API. Security of API affect the security and availability of cloud services strongly [27]. Safe APIs guarantee protected and non-destructive use of cloud services [11]. An API can be considered as a user guide for describe details of cloud service providers and cloud architecture and features. Users build and develop services with API [27]. Usually, Cloud service providers release their APIs for marketing their cloud. On the one hand, publishing API helps users to become aware of the detail of components and cloud performance. On the other hand, the cloud architecture is somewhat exposed to invaders [27]. So, unsafe API can be problematic for users and users. API vulnerabilities include weak mandate, insufficient authorization and input data authentication. In addition, frequent updates to the API may create security holes in programs [14].

4.Identity management and access control solutions

Access control and identity management are intensity required in the cloud in order to make cloud computing the acceptable for the society as cloud security union states. The Cloud Security Union offers following key points to control identity and access control. Open standard federations, such as SAML and OAuth, should be preferred, if possible.
Sources attribute should be as close as possible to the master source.
All institutions features should have an identified level of trust.
Mutual trust should be ensured for secure relationships and transactions.
Services should import or send functions using standards like XACML and OASIS.
The attribute-based encryption [ABE] is used to provide access control in the cloud that has been trading access control policies are set and implemented. ABE has been introduced in [17] and uses encrypted messages that use traits, combined and decrypted by the users who run it have traits. Encryption is based on the set of traits [ASBE] [3], the developed method is ABE and user attribute to the recursive set-based classification of cosmetics, and allows users to apply the dynamic adverbs on how those attributes, access control policies are mutually run. The authors in the reference [26] extended ASBE to encrypt based on a hierarchical set of traits that development of [HASBE] hierarchical user structure. A series of HASBE to users with a valid reference to the root level, in terms of reference. Valid references to domain level and subsequently in the next step, where users or affiliate domain references within the management domain. By domain or subdomain, page references to users can be trusted as sources for this case, there is also a hierarchy. Master key system parameters reference, the authoritative root, and domain distribution for references. The keys are generated using mutual cross groups. The parameter of the system, including system parameters to build the groups. Private/public keys for users by domain references are exported, hierarchical tree structures associated with elements that are elements of a trait or a set of attributes. Access control is also defined as a hierarchical tree structure. The data encryption key has encrypted the data. Data encryption key of the Cal optima privacy HASBE structure uses the access key; this structure, attributes, and access control policies. The expiration time to access the key structure for the purposes of the user can be added to the revocation. Access to the decryption can be granted to users that the traits and existing policies in the structure. To control access, HASBE to reassure cloud data. Figure 5 system models for HASBE offers. Ruj and colleagues [16] is a method of non-controlled central authentication and access to cloud storage offer. This method of trait-based signature and ABE [ABS], arrange for anonymous access and authentication control. Anonymous authentication, user authentication without exposing the identity of a user, allowing. Signature, based on attributes, processing, and verification that the identity or the need for authentication process disappears. This method uses the third person sure has issued lists for users. The user codes to a key distribution center [KDC]. KDC encryption/decryption keys and signatures based on bi-directional pair up. The user data encrypted and signed, and then sends to the cloud. The cloud attribute on the basis of the signature is verified and the data in case of a valid user. Annulment of the user by changing the parameters of the data encryption that has similar characteristics with the attributes of the user are revoked. The authors in the reference [25] a few proprietary access control methods based on role [RB_MTAC] suggested that this approach identity management and access control of the role-based compound. This method needs to be registered by users of a specific ID, and cloud. The user password during the registration process. To enter the cloud, a user must have a user identity management module based on the validity of the registered identity detection, pass. After authentication, the user's role assignment module which is connected to the database of RB_MTAC, and sent to the user based on information recorded plays. All resources via the RB_MTAC module access control list resources, available to the user. The authors in the reference [5] is a digital identity management system called ' privacy with identity management for cloud environment ' [SPICE]. SPICE of random and signature concept for providing anonymous authentication [the authentication for the user without exposing its

Table 9: Identity management and access control strategy

Research	suggested method	Basic theory	Security Features	Scalability
[26]	HASBE, Method of access control for cloud	-Encryption based on the category attributes -Hierarchy of trust	Control access - to storage in the cloud -User annulment Re-encoding - Privacy -	High
[16]	Decentralized access control for storage in the cloud	Pairing two- - way Encryption - based on attribute Members based on attribute	-User authentication Control access - to storage in the cloud	Mediocre
[30]	Role-based access control method	Role-based - access control	-Control access to cloud resources	Low
[5]	SPICE, Identity Management Framework	-Anonymous and representable authentication -Ability to lack of communication - Accountability - Access Control	- Signatures group - Randomization	High
[1]	Identity Management Framework	-User Managed Access Protocol	- Identity Management Authentication - Access Control -	Low

identity], lack of communication, the ability to delegate authentication [cloud service providers are not allowed a user's transactions related to each

other], answering the central control and user accessibility. In addition to the SPICE all features listed with just one registration provides. Registered user and be sure the name of the section by a Registrar, a certificate for all the services provided by cloud services providers have been provided. Achieved through user authentication, a certificate of authentication. Since the cloud service providers are different, different traits need for authentication, the user can have different versions of the authentication certificate from a certificate name. Group signatures on certificates are used for authentication. The signature SPICE Waters [25] and the Groth_Sahai degree [7] for the signature of group development. The signature of the user, through a group guarantee that the signature of the parties to a valid user of a group that needs to be guaranteed, the identity. For random signatures to create more lack of communication, has been applied. The random building also had to hide a specific cloud service providers do not need to use it. Dhungana et al. [1] propose the identity management framework for cloud network infrastructure on which the managed user access protocol [UMA] focused. Under construction in this procedure as permission Manager [AM] will be considered. Cloud service providers such as a host while the owners of the service such as licensed users are considered. The services are controlled by the AM. The nature of the users who are applying is also managed by the AM. Any services requested by AM which can be checked in accordance with the access control policy, accept or reject. The proposed framework can access control and identity during the cloud service providers are numerous, the AM for providing services for identity management and access control are coordinated together. The points relating to the procedure provided in table 9 have been brought.

Table 9: Identity management and access control strategy

5.The security solutions for cloud applications and API's

Cloud and API programs of SaaS and SaaS layers need special security concern for the safety during the life cycle performance and development. Cloud Security Alliance [21] suggests that security for cloud apps and API should be provided without any assumptions about the external environment .Then, the Cloud Security Alliance's main recommendations about Cloud and API programs are offered.

- Privacy and security requirements [functional and supervision] should be defined according to the needs of the expanding cloud. Buyers should also be defined in terms of effect and the possibility of them listed.
- Threats and attack vectors that are for cloud computing, should be checked and Homogenized with the security requirements. Risk and attack models should be continuously developed and updated.
- Secure cycle software development and software architecture must be developed and updated.
- Software components with the ability to reuse and are well-known to reduce the security and breach scenarios, should be used.

Table 7: Comparison of proposed methods for safe storage in the cloud

Research	Suggested method	Basic theory	Privacy	Integration	accessibility	Scalability	Other Features
[24]	SecCloud and a storage protocol for security and privacy	- Associated bilateral - Signature verification - Encryption	✓	✓	×	mediocre	Audit computing
[19]	One way to secure static data	SSL Symmetric encryption	✓	✓	✓	Low	- Access Control - Encryption Search
[23]	One way to secure static data	- Axis correction code - Redundancy of data	✓	×	✓	mediocre	- Secure against Byzantine errors - Secure against collusion Server
[22]	FADE a protocol for privacy and data integrity	- Encryption - Reliable third party - Remove reliable - Threshold secret sharing	✓	✓	×	High	- Access Control - reliable Remove
[15]	Time PRE a secure method for sharing data in the cloud	-Re-encoding Proxy - Encryption based on attributes	×	✓	×	mediocre	Access Control

Table 8: Comparison of the proposed strategy for the security of cloud applications and API's

research	suggested method	Basic theory	Security Features	Scalability
[20]	Control access for cloud applications	-Diameter protocol	- Authentication - License -Accounting [check authenticity]	high
[1]	A method to ensure the integrity of applications in the cloud	-Reliable platform module Elliptic - curve cryptography	-Program Integrity -Integration Platform	Low
[45]	Security as a service for cloud apps	Security as - a service in the cloud	- Clouds recommended by security services	Low
[21]	API management platform for secure cloud APIs	Free license - on the basis of a password	Access - Control	mediocre

- Regular penetration testing should be done for web applications.
- To ensure the safe management Session for Web applications, manual testing should be performed periodically.

To protect the Cloud program from unauthorized access, writers in reference [20] suggested using Diameter_AAA protocol. This protocol uses network-based access control for filtering unauthorized access requests to cloud applications. All requests that are initially sent to network access server, are sent to the server diameter. The server checks authentication and authorization parameters and based on the results, requested access to applications will be accepted or rejected. Diameter protocol in addition to the authentication and authorization, also provides accounting services to the cloud. Alowolodu and colleagues [6] proposed the use of TPM and elliptic curve cryptography [ECC] to provide a secure platform for application performance in the cloud. Keys are generated Using ECC and stored in the TPM configuration registers. Platform Integration guaranteed before transfer programs to it. It also uses recommends encryption when transferring applications between platforms. Program Integrity platform is controlled prior to its implementation. The authors in reference [45] offered providing security as a service [SECaas] in a cloud environment. SECaas recommends the security services that are provided by various clouds and an independent cloud [cloud management] that track these services. The user defines the security requirements for cloud management and cloud management identifies clouds offer that services. The user program is recorded by Clouds provide security that provide security. SECaas works at all levels [SaaS, Paas, IaaS] and

makes services safe. Reference [21] recommends a cloud API management platform that provides access control architecture for cloud API. The access control in proposed platform is based on OAuth [Open Authorization] that is password-based access control mechanism. Password-based access control uses password instead of user credentials to access its resources. Programs can use a password instead of User. In this way, the provider records API and releases API with API's management platform and acquires a key validation codes and acquires a key for validation codes. API's consumer request to access password from API management platform. After validation request a key is given a key to it. Both key issued to the provider and consumer are personal keys. Consumer using a code that is marked request with his own key to the API. Provider sends password to API management platform for authentication and if it was valid it will be placed in the hands of the consumer. Table 8 shows a summary of the proposed method.

6.Conclusion

Cloud security risks in the cloud may differ with risks of traditional information technology, whether in nature or intensity, or both. The shared use of resources allows a lot of users to use a similar source that is possible through several proprietary virtualization and technologies. In this paper, we described challenges based on the two areas as follows: [A] identity management and access control, [B] security of Web applications and applications programming interfaces. And also we compared existing solutions in order to upgrade security at these two level.

References

[1] O.D. Alowolodu, B.K. Alese, A.O. Adetunmbi, O.S. Adewale, O.S. Ogundele, Elliptic curve cryptography for securing cloud computing applications, Int. J.Comput. Appl. 66 [2013].

[2]R. Bhadauria, R. Borgohain, A. Biswas, S. Sanyal, Secure Authentication of Cloud Data Mining API, arXiv preprint arXiv:1308.0824, 2013.

[3]] R. Bobba, H. Khurana, M. Prabhakaran, Attribute-sets: a practically motivated enhancement to attribute-based encryption, in: Computer Security ESORICS, Springer, Berlin, Heidelberg, 2009, pp. 587–604.

[4] S. Carlin, K. Curran, Cloud computing security, Int. J. Ambient Comput. Intell. 3 [1] [2011] 14–19.

[5] S.M.S. Chow, Y. He, L.C.K. Hui, S.M. Yiu, Spicesimple privacy-preserving identity-management for cloud environment, in: Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, 2012, pp. 526–543.

[6] R.D. Dhungana, A. Mohammad, A. Sharma, I. Schoen, Identity management framework for cloud networking infrastructure, in: IEEE International Conference on Innovations in Information Technology [IIT], 2013, pp. 13–17.

[7]] J. Groth, Amit Sahai, Efficient non-interactive proof systems for bilinear groups, in: Advances in Cryptology EUROCRYPT, Springer, Berlin, Heidelberg, 2008, pp. 415–432.

[8] Q. Duan, Y. Yan, A.V. Vasilakos, A survey on service-oriented network virtualization toward convergence of networking and cloud computing, IEEE Trans. Netw. Service Manage. 9 [4] [2012] 373–317.

[9] B. Guan, J. Wu, Y. Wang, S.U. Khan, CIVSched: a communication-aware inter-VM scheduling technique for decreased network latency between collocated VMs, IEEE Trans. Cloud Comput. 2 [3] [2014] 320–332.

[10] T. Jung, X. Li, Z. Wan, M. Wan, Control cloud data access privilege and anonymity with fully anonymous attribute based encryption, IEEE Trans. Inform. Forensics Sec. 10 [1] [2014] 190–199.

[11] R. Latif, H. Abbas, S. Assar, Q. Ali, Cloud computing risk assessment: a systematic literature review, in: Future Information Technology, Springer, Berlin, Heidelberg, 2014, pp. 285–295.

[12] M.J.Hosseinpoor, M.zolfpour- Arokhlo, An investigation in cloud computing security: problems and challenges, International Journal of Scientific & Engineering Research, Volume 6, Issue 8, August-2015 PP. 1522-1527.

[13] W.A. Jansen, Cloud hooks: Security and privacy issues in cloud computing, in: 44th Hawaii International Conference on System Sciences [HICSS], 2011, pp. 1–10.

[14] Hosseinpoor.,MJ., Rezvani., F., Sajadi., S., " Comparative Load Balancing Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Engineering & technology, Volume 6, Issue 2, February 2017.PP. 183-187.

[15] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inform. Sci. 258 [2014] 95–318.

[16] S. Ruj, M. Stojmenovic, A. Nayak, Decentralized access control with anonymous authentication of data stored in clouds, IEEE Trans. Parallel Distrib. Syst. 25 [2] [2014] 384–394.