Security Issues and Solutions in Cloud Computing

29/April/2019

Jeffry Rochili: 12093783
Eda Ye: 12445995
Beomsang Kim: 13340106

Abstract

Cloud computing is most notable technology in current IT industry. It has been adopting in many organisations and individuals. However, the state of cloud security has been evolving throughout the years which corresponds to the changes in the hardware department. These changes brought new challenges to the core security problem such as privacy, policy and authentication. In this paper, we identify some of the issues that cloud environment face, examining the possible solutions that are commonly used and their advantages.

Keywords

Authentication, Encryption, Management, Security

Background

Cloud computing has been steadily growing its market and influence throughout the enterprise business as an alternative to traditional IT architecture. Either self managed or third party, cloud services has been proven to have advantages in both scalability and cost efficiency. Enterprises have been migrating their data into data centers in recent decades, observable from the massive growth rate of third parties cloud service providers such as Amazon AWS and Microsoft Azure.

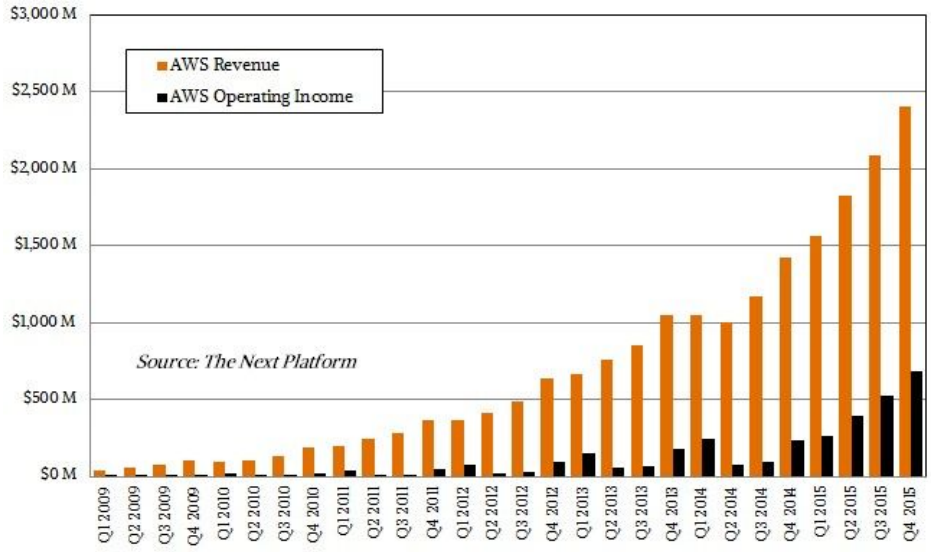

Figure 1. Amazon AWS growth chart (Morgan 2016)

Figure 1 shows that Amazon had made great investment and revenue in developing its AWS, showcasing market demand and feasibility. However, there are various challenges that threaten cloud security and the data stored in these systems.

Privacy

The privacy issue is the most important security part of cloud computing. Cloud computer can contain end users' sensitive personal details and allow data transmission. There is a high probability that intruders can attack the information. Jajayatchumy et al. (2010 cited in Zargari and Smith 2014, p. 150) announced that information in a cloud computing system has five different types.

- 'Personally identifiable information': this information can be directly traceable user information (name or address) or indirectly notable information of the end users (credit card number, postal code)

- ‘Sensitive information’: private information which requires more concern such as religion, race, health or sexual information.

- ‘Information considered being sensitive’: Biometric information or close observation image in public.

- ‘Usage data’: the users’ data added by computer devices like web site visitation history.

- ‘Unique device identities’: Unique and notable information of devices such as IP address.

If cloud provider cannot protect end users’ privacy, the end users will not trust cloud provider. Therefore, lack of trust is an important privacy challenge in the business side of view. If the cloud provider serves excellent privacy protection combines other high-security protections, and it gives positive brand image and trust to consumers (Sharma and Gupta 2013, p. 138 -139). Trust leads to more economic benefits for cloud providers and sustainability.

Policy

Policy worries are raised with the development of cloud computing. Many policies are involved in cloud computing. The policies can be technical standards like bigtable in Google or Hbase in Yahoo (Liu et al., 2012, p. 274), business policies, operation policies or public policies. However, wrong or inappropriate policies can lead to security issues. For example, an organisation can reduce weight to physical security to saving their budget and invest in other business activities. That policy can lead to physical penetration form intruder. Also, there is an ambiguity in the relationship in public policy and technical ability. Cloud providers can only assure limited security from government surveillance and data collection (Jaeger et al., 2008, p. 278).

Moreover, Jaeger et al. (2008, p. 278) state that information policy in the United States cannot follow the current speed of technology development. Old public policies cannot handle new technical problems and expectations. Moreover, those policies can interrupt technical development. Clear policies are required in cloud computing.

Data Security

Cloud computing is an approach to store the database and software resources in large data centers, and it also provides fast computing (Sandeep K.Sood, 2012, p. 1831). As cloud consumers cannot directly participate in the management and maintenance of data, the protection of data is a big issue for cloud computing. Three cryptographic parameters are used to measure the security of data: Confidentiality, Availability and Integrity(Sandeep K.Sood, 2012, p. 1831).

- Confidentiality: Only authorized people, resources, processes are permitted to operate the data
- Availability: The data or software resources is available for authorized people when needed
- Integrity: Preventing data from being intentionally or accidentally changed

The protection of data can be achieved based on the three aspects.

Solutions

IDMs for Privacy Protection

Appropriate solutions are needed for secure privacy in cloud computing. Sen (2018, p.31) states that 'privacy-protection mechanisms' have to consider in all cloud security solutions. Identity Management (IDM) is required for authentication. IDM supports user authentication in cloud computing. IDM has accompanied with IT progression, cluster computing and Peer-to-Peer systems which now changed into cloud computing (Slone 2004; Youseff et al. 2008 cited in Habiba et al 2014 p. 5). IDM has various of subtypes.

Deployment based classification

Deployment based classification contains isolated, centralised or federated IDM structure (Habiba et al. 2014 p. 6). The classification usually hands with underlying architecture for storage, management and identity information flow (Habiba et al. 2014 p. 6). The identity information can be contained in single or distributed servers (Habiba et al. 2014 p. 6).

Isolated Cloud IDMS

This IDM system method is used by the small or medium organisation (Habiba et al. 2014 p. 6). In this case, single server conducts as Service Provider (SP) and Identity Provider (IdP) which has responsibility for the identity information and user operations storage (Alrodhan and Mitchell 2010; Cao and Yang 2010; Jøsang et al. 2005 cited in Habiba et al. 2014 p. 6). If a user requests authentication, cloud provider turns request to own IdP for verification. After successful

verification, the cloud provider response to the user. Isolated Cloud IDM does not need Trusted Third Part for verification (Habiba et al. 2014 p. 6).

Centralised Cloud IDMS

The centralised Cloud IDMS serrates SP and IdP's function (Habiba et al. 2014 p. 6). Single IdP manages issuance, storage and identity data (Cao and Yang 2010; Jøsang et al. 2005; Windley 2005 cited in Habiba et al. 2014 p. 6-7). The IdP accumulates identity information from a cloud provider (Habiba et al. 2014 p. 7). This IDM redirects authentication requests to the related IdP. After processing, the cloud provider will get request and response to the user who requested.

Federated Cloud IDMS:

This system currently gets attention because it is designed to permits cross-domain access to users for without requirement for extra user accounts for external parties (Arias-Cabarcos et al. 2012; Shin et al. 2009; Suriadi et al. 2009 cited in Habiba et al. 2014 p. 7). Federated IDMS stores identity information in multiple storages (Habiba et al. 2014 p. 7). Two cloud providers are involved in authentication. When an authentication request is generated, cloud provider one acts Federated Cloud IDMS and delivers to cloud provider two for collecting user identity credentials. Cloud provider two sends the request to the next IdP and reclaims necessary attributes from an identity data store. Authentication response will be generated after the process and sent to cloud providers.

User-Centric IDMS

User-Centric IDMS can be established on federated IDMS or centralised IDMS for management and identity credential storage (Habiba et al. 2014 p. 8). User-centricity and Anonymity are part of User-Centric IDMS.

User-Centric Cloud IDMS

This IDMS joins all user identity provisioning transactions (Habiba et al. 2014 p. 8). When user requests authentication, IdP reply to with all need credentials for authentication (Habiba et al. 2014 p. 8). In this system, storage, management and retrieval are mandatory to the user for identity credentials (Habiba et al. 2014 p. 8). Also, the user decides identity credential trade with other credible entities (Habiba et al. 2014 p. 8).

Anonymous Cloud IDMS:

The Anonymous Cloud IDMS can keep its owner's secret from any others (Bhargav-Spantzel et al. 2007; Conrado et al. 2003; McCallister 2010 cited in Habiba et al. 2014 p. 9). This IDMS is useful when lack of trust is involved between user and cloud providers (Habiba et al. 2014 p. 8).

Secure Policies

Security policies can be different depends on cloud computing services, IaaS, PaaS and SaaS. Three different cloud services provide a unique service to users. Also, they have unique technical features. Therefore, the three services need different policies. Zhu et al.(2012, p. 416-417) suggest policies for each types.

Security policies for IaaS

IaaS needs the following security policies to protect the data centre.

- Physical environment safety: The policy can be implementing camera, biometric, card readers and alarm system

- 'Network and host security': Firewall, antivirus program, load balancer and intrusion detraction are the examples for against Denial of Service (Dos) attack. Also, the network management team must implement Access Control Lists (ACL) for a virtual local network segment and applications.

- Service continuity: security policy must concern data protection and system.

Security policies for PaaS

PaaS allows users to develop their software without management and controls. Therefore, the following policies are mandatory.

- IDM

- Information Protection: Cloud providers must consider avoiding accidental data leakage, secure transmission, funning platform protection and integrity system.

Security policies for SaaS

SaaS gives many applications for users. Following suggestions are necessary for SaaS.

- Engineering safety: This policy considered all platform design stages system.

- Secure framework design of applications: Auditing, authentication, authorisation, communication, configuration, algorithm, sensitive data and validation are considered.

Proposed Framework

There is a proposed framework being structured to provide the security of data. It is divided into two phases, one deals with the process of storing data, while another one is for retrieving data. Phase 1 consists of many sub sections: Classification, Encryption and Message Authentication Code(MAC). While phase 2 focus on IDM mentioned above.

Classification

The data should be stored in different sections (public, private, limited access) based on three cryptographic parameters mentioned above. The value of these parameters will be listed by client himself and sensitivity rating(SR) will be calculated with a proposed algorithm. The value of Confidentiality is based on the privacy level when processing data; the value of Availability is based on the frequency of accessing data and when requested the data should be available immediately; the value of integrity is based on the accuracy of data, reliability of information and eradication of unauthorized modification. The formula to calculate SR is SR[i] = (C[i] + (1/A[i])*10 + I[i]) / 2 . After the SR is calculated, the data will be allocated in different sections based on it.

Encryption

Encryption is the process of turning intelligible information into useless information (Sandeep K.Sood, 2012, p. 1831). There are some mechanisms to help encrypt the stored data. A key of fixed length is used to encrypt the data with some hash functions. Encrypted data is more secure, even it is stolen, it is almost impossible to acquire useful information without the hash function and the key. In addition, searching over encrypted data is complicated, as a result, a index builder is used to create a index for the data, and the index should also be encrypted.

Advanced Encryption Standard

Advanced Encryption Standard (AES) is one of the more common and secure encryption method implemented as of this moment. It is a block cipher that could use either symmetric or public key for secure encryption method (Rawal 2016). Rawal (2016) noted that a practical attack method against AES has yet to be discovered, albeit when properly implemented.

Message Authentication Code

MAC is a small fixed size block of data generated based on message of variable length using any secret key (Sandeep K.Sood, 2012, p. 1831). It will be generated and transmitted to cloud with encrypted data together.

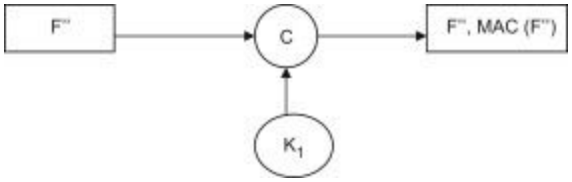

Figure 2: The workflow of MAC(Sandeep K.Sood, 2012, p. 1831)

The picture above illustrate the workflow of the MAC. A MAC is generated for the file F'' use the key K1, then the file data and the MAC is transmitted to the other side. It can be used to check whether there is any modification when transmitting the data, which is a protection of integrity of the data.

Identity and Access Management (IAM)

It is common knowledge that user/client information is one of the most crucial aspect in cloud security, however it also requires the users and account owner to be responsible on their part too. The dangers that threaten ranges from common recklessness such as using easily guessed or weak password combination, or intrusion in the form of data/packet monitoring. Authentication and authorization are often mentioned together but it differentiates the user entity and its ability to access allocated content resources (Google Cloud 2019). Their connection is often confused as the difference are less observable when the new identity and access level are created, distributed and revoked many times to individuals both within and outside an organization (Dotson 2019). Dotson (2019) describes how a person could reduce security risk by minimizing the number of people and organization involved or put trust in.

Here are some of the common solution often implemented:

1. Logging could be used to monitor and document data access. By documenting the connection source detail and changes made, notifying admins when sensitive information is accessed or tempered with.

2. Two-factor access is an ergonomic method to provide another line of defense in case of lost credential which could create high impact consequences. This method requires the user knowledge (password) and possession (phone) for authorization.

3. Using cloud IAM service (Amazon IAM) or Identity-as-a-Service (IDaaS) for ID management system (Amazon Cognito).

Authorization

To manage resource access there has to be an authorization process. Access control policies or access right delegation could be used in cloud environment (Indu et al. 2018). Role or attribute based access control are common access control policies used to segment various level of security clearance granted to groups or individuals. However, when access is configured poorly such as creating a public access to a cloud database, the fault lies on the engineers. In 2017, the Election Systems & Software backlash causes data leak that exposes personal information of voters in Chicago to the internet (Goud 2017).

Revalidate

Revalidating users for automating the authentication and authorization process is important the implementation of the core system design. In cloud environments, revalidation may have limited control and therefore should be checked periodically to ensure that they are still valid for their access privilege (Dotson 2019). There is risk such as past employees still retaining access to the organization. The process would also help to regularly clear out outdated access accumulated by the system.

Summary

Privacy issues are important security issues in cloud computing. The issues can make business problem to cloud providers. IDM is suitable solution for protect user privacy. It supports user authentication in different types of technical methods. However, authentication is not only considered aspect. IDM cannot guarantees availability and integrity. Encryption is commonly used to protect the confidentiality of user data. Identity and access management are key aspects in the authentication process which segregates the identity and the its authorization to various degree of resources. Revalidation has to be done seamlessly to allow automation process.

Policy issues are directly affects cloud computing security management and development. The report suggested secure policies for each types of cloud computing systems, but detailed technical suggestions were not written and not covered public policy issue.

References

Dotson, C. 2019, 'Practical Cloud Security', *O'Reilly Media*, electronic book, viewed 27 April 2019, <https://learning.oreilly.com/library/view/practical-cloud-security/9781492037507/?ar>.

Google Cloud 2019, *Authentication Overview*, viewed 27 April 2019, <https://cloud.google.com/docs/authentication/>.

Goud, N. 2017, 'Top 5 Cloud Security related Data Breaches!', *Cybersecurity insiders*, viewed 28 April 2019, <https://www.cybersecurity-insiders.com/top-5-cloud-security-related-data-breaches/>.

Habiba, U., Masood, Rahat., Shibli, M. & Niazi, M. 2014 'Cloud identity management security issues & solutions: a taxonomy', *Complex Adaptive Systems Modeling*, vol. 6, no. 6, pp. 2:5.

Indu, P. M., Anand, R., & Bhaskar, V. 2018, 'Identity and access management in cloud environment: Mechanisms and challenges', *Engineering Science and Technology, an International Journal*, Vol 21, Issue 4, pp. 574-588, viewed 27 April 2019, <https://www.sciencedirect.com/science/article/pii/S2215098617316750>.

Jaeger, P., Lin, J. & Grimes J. 2008 'Cloud computing and information policy: computing in a policy cloud?', *Journal of Information Technology & Politics*, voi 5, no. 3, pp. 269-283

Liu, C., Chen, W. & Tung E. 2012, 'Identification of critical security issues for cloud computing', *Applied Mechanics and Materials* , vol. 145, pp. 272-276

Morgan, T. P. 2016, 'HOW LONG CAN AWS KEEP CLIMBING ITS STEEP GROWTH CURVE?', *The Next Platform*, viewed 29 April 2019, <https://www.nextplatform.com/2016/02/01/how-long-can-aws-keep-climbing-its-steep-growth-curve/>.

Rawal, S. 2016, 'Advanced Encryption Standard (AES) and It's Working', *International Research Journal of Engineering and Technology (IRJET)*, vol. 3, issue 8, pp. 1165-1169, <https://www.irjet.net/archives/V3/i8/IRJET-V3I8214.pdf>.

Sandeep K.Sood, November 2012, 'A combined approach to ensure data security in cloud computing', Journal of Network and Computer Applications, vol. 35, pp. 1831-1838

Sen, J. 2014 'Security and privacy issues in cloud computing', Architectures and Protocols for Secure Information Technology Infrastructures, IGI Global, Pennsylvania.

Sharma, P. & Gupta, P. 2013, 'Survey on cloud computing security policies and privacy concerns for information security' , *International Journal of Advanced Research in Computer Science,* vol. 4, no. 11, pp. 134-142.

Zargari, S & Smith, A. 2014, 'Policing as a service in the cloud', *Information Security Journal: A Global Perspective,* vol. 23, no. 4-6 pp.148-158.

Zhu, Y., Liu, P. & Wang, J. 2012, 'Cloud security research in Cloud Computing', *Applied Mechanics and Materials,* vol. 198-199, pp. 415-419