Cloud Security: An Overview and Current Trend

P. K. Paul[1] & P. S. Aithal[2]

[1]Executive Director, MCIS, Department of CIS, Raiganj University (RGU), West Bengal, India

[2]Vice Chancellor, Srinivas University, Karnataka, India

E-mail: pkpaul.infotech@gmail.com

Type of the Paper: Research Overview.
Subject Area: Information Technology.
Type of Review: Peer Reviewed.
Indexed In: OpenAIRE.
DOI: http://doi.org/10.5281/zenodo.3514577.
Google Scholar Citation: IJAEML

How to Cite this Paper:

Paul, P. K., & Aithal, P. S. (2019). Cloud Security: An Overview and Current Trend. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *3*(2), 53-58. DOI:http://doi.org/10.5281/zenodo.3514577.

International Journal of Applied Engineering and Management Letters(IJAEML)

A Refereed International Journal of Srinivas University,India.

IFSIJ Journal Impact Factor for 2019-20 = 4.252

Cloud Security: An Overview and Current Trend

P. K. Paul[1] & P. S. Aithal[2]

[1]Executive Director, MCIS, Department of CIS, Raiganj University (RGU), West Bengal, India

[2]Vice Chancellor, Srinivas University, Karnataka, India

E-mail:pkpaul.infotech@gmail.com

ABSTRACT

Cloud security is also called as cloud computing security. It is the set of policies, technologies, applications, and control utilized for virtual infrastructure which includes hardware, software, and application. The field is closely related to database security, web security, network security, etc. In other words, cloud security is very close to computer security, IT security or information security. Day by day the IT infrastructure becomes a common need of every individual and organization so the security aspect is an important concern in this regard. Cloud computing security is controlled by different mechanisms such as deterrent control, preventive control, detective control, and collective control. Cloud Vulnerability and Penetrating Testing are very much important for secure and healthy cloud security practices. Cloud Computing is an important name in the IT and Computing domain and this is rising in different organizations and institutions. In this paper different areas of Cloud Computing have been described. There are different models and architecture for cloud computing security and different rules, regulation, and framework. This paper is conceptual in nature and talks about various areas of security in the basic sense. Paper also talks about Security affairs related to the Cloud.

Keywords: Cloud Computing, IT Security, Virtualization, Cloud Security, Mobile Security, Current IT Trends.

1. INTRODUCTION :

Cloud computing security is majorly consisting with data security part. It is important to note that encryption is also very important for cloud computing data security and privacy. There are different rules and regulation and framework for better cloud security [1], [5], [9]. Cloud Computing Security is also referred simply as Cloud Security, it is the way, techniques, procedure to protecting data and contents from the online systems. In generally Cloud Security may be a solution from the leakage, deletion of the data and among the popular methods of keeping cloud systems or online systems safe few important are include—

- Use of firewall;
- Penetration testing;
- Use VPN only in real need;
- Tokenization
- Avoiding public internet systems etc [2], [3], [18].

Apart from these more are required for the healthy and sophisticated IT infrastructure development. There are different threats in Cloud Security and among these important are data breaches, loss of the data, insecure APIs, Poor Cloud Service Providers, Distributed Denial of Service attacks are also important [4], [6], [7].

2. OBJECTIVE AND AGENDA :

The main aim of this paper includes but not limited to the following—

- To learn about the basics of Cloud Computing and its types, nature as well as importance.
- To know about the fundamentals of Cloud Computing Security or Cloud Security with importance.
- To learn about the basics of Cloud Security Threats and their continuous development.
- To learn about the fundamentals of Cloud Security threat management tools as well as ways.

- To learn about the different Cloud Security Controls and Security and Privacy issues in brief manner.
- To learn about various Encryption methods that may be applied in Cloud Security management.

3. CLOUD SECURITY: THE ROOT :

Cloud Security is also treated as Cloud Computing Security and it is very close with the Network Security, Database Security, Web Security etc. Moreover, it is very close with the Information Technology Security [8], [10]. Cloud Security is important in generally concerned within the secure, safe data and contents in the cloud systems. Additionally, security is needed in all the modes and platform in cloud computing. Cloud Computing is the virtualization of IT Infrastructure which include the software, hardware, network, websystems etc. And this may be availed or designed and developed by the following models—

Public Cloud Computing—It is the creation and doing IT Infrastructure virtually from the remote places using appropriate (internet based) technologies.

Private Cloud Computing—It is the designing, development of own Cloud based infrastructure into their territory without third party.

Hybrid Cloud Computing—It is the combining both i.e., Public Cloud and Private Cloud Computing and uses based on need.

Hence in all these three models, security concept should be provided and these are increasing day by day due to the growing IT usages. And Cloud Computing services are offered as Software-as-a-Service, Security-as-a-Service, Storage-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service. And all these services are offered by the online systems to the client and thus proper mechanism is very important for the security related affairs [11], [16].

Though sometimes it may be noted that due to requirement of the more security in the data management companies are using cloud based service providers and sometimes they are using security services of the cloud computing with the believe that cloud service provider can store their data safely and with proper measures and whereas inside the company or local servers vulnerability is an issue.

4. CLOUD COMPUTING ANDATTACKS :

Cloud Security is an important concern as various means are required for its various facets viz. Public Cloud Computing Security, Private Cloud Computing Security, Hybrid Cloud Computing Security [12], [13]. Moreover, Security is needed in following deployment models as well—

- Security in Software-as-a-Service,
- Security in Security-as-a-Service,
- Security in Storage-as-a-Service,
- Security in Platform-as-a-Service,
- Security in Infrastructure-as-a-Service etc.

Hence for healthy and proper Cloud Computing practices few things are very important and among these important are appropriate firewall. With PaaS, client basically creates applications with the programming languages as well as tools provided and supported by the vendor and then it is required to deploy these to the cloud infrastructure. “With IaaS, there are few integrated security capabilities beyond protecting the infrastructure itself, but there's enormous extensibility”, *according to the CSA*. Actually, Cloud Security is the concern of two sides—

- ***Firstly,*** the Service Providers of the Cloud Computing i.e. the vendors of Cloud Computing
- ***Secondly,*** the Service Seekers of the Cloud Computing i.e. the client or the customers of the cloud.

In Cloud, it is essential to confirm that the service providers should ensure they have with inbuilt security services and also from user’s perspective, proper attention paid on the system. Inside attacks are very important in cloud computing, according to a study it has been noted that sixth biggest threat on cloud security is from the inside attackers [14], [15]. Data isolation and logical storage segregation is very important for cloud security as normally Cloud Security providers offers services to the multiple users and with this model one provider can serve many. As a result, Data isolation is important. Sometime competitors try to follow others data. Hence solution is required in this context [17], [19].

Virtualization alters the relationship between the OS and underlying hardware and thus security concern is very important in many cases. Hence for this additional layer proper security must be provided.
Cloud Vulnerability and Penetration Testing is also very important concern in sophisticated Cloud Security prevention. Scanning the Cloud Systems from the inside and outside also very important and required for managing from the data leakage, malware etc. [20], [21].

5. SECURITY MANAGEMENT &CLOUD :

Cloud Security is possibly managed by the different sources and ways and among these few important are include—

Cloud Security Controls—

A proper security is only possible to bring by the proper and appropriate systems and in this regard, effective controls are very important. Among the effective control following are important—

- Deterrent Control (typically reduce the threat level by informing potential attackers)
- Preventive Control (It is responsible for strengthening the system against incidents, generally by reducing threats if not actually eliminating vulnerabilities)
- Detective Control (Detective controls are intended to detect and react appropriately to any incidents that occur)
- Corrective Control (Corrective controls reduce the consequences of an incident, normally by the limiting the damage) [13], [22], [23]

Encryption Techniques—

In healthy Cloud Security practice proper encryption techniques are very important and especially crypto-shredding. This is the designing of appropriate algorithm to prevent the cloud systems. Some of the encryption model and algorithms are include—

- Attribute-based encryption (ABE)
- Ciphertext-policy ABE (CP-ABE)
- Key-policy ABE (KP-ABE)
- Fully homomorphic encryption (FHE)
- Searchable encryption (SE)

Privacy and Security: Techno-Managerial—

For healthy and sophisticated Cloud Security practice following are important and these should be brought both by the cloud service providers and cloud service seekers as well. Following are the requisite for the privacy and security management—

- ***Identity Management*** (Identity management system is very important for the healthy and smart cloud services, here users should have proper identification systems and for this biometric system can be installed. Moreover,CloudID may also introduced for privacy-preserving cloud-based and cross-enterprise biometric identification. With appropriate identification systems the chances of attacks may reduce radically)
- ***Physical Management***(Cloud Computing service providers normally maintain their security of the equipment, tools, products, servers etc from the unauthorized access, including the interference, theft, fires, floods, some other natural disaster etc)
- ***Personal Security***(Many professionals normally manages the cloud based systems as an employee and thus pre training is important for better security. Moreover, all the employees may not associate with the organizations and thus for future security this should be keep in mind)
- ***Privacy Security***(All the credentials, data etc should be keep in a secret place or proper strategy should be employed)

This way, Cloud security may be ensured by the both cloud service providers and cloud computing service seekers as well. And based on organization, types and situation the cloud computing security strategy may be changed [20], [24].

6. SECURITY POLICY: THE WAY :

Cloud Security with sophisticated way is possible to maintain and thus the policies may vary service providers to service providers or even client to client. Based on the service model also security policy may be differed. In generally, Cloud Security policies may be different on your types and deployment models, details are depicted in Table: 1.

Table1: Security Policies in Cloud

Security Policies respect of Deployment Models	Different Types of Cloud and Policies
Security Policies in Software-as-a-Service Security Policies in Security-as-a-Service Security Policies in Storage-as-a-Service Security Policies in Platform-as-a-Service Security Policies in Infrastructure-as-a-Service etc.	Public Cloud Computing Policies Private Cloud Computing Policies Hybrid Cloud Computing Policies

Cloud Security needs majorly for the storage and thus proper security must be ready for the better and effective services. Third-party audits of a cloud provider's security systems also very important in various cases. Additionally, Cloud users must protect access from the unauthorized credentials, log-ins, persons etc. Moreover, data stored on a cloud-hosted in different nation may have different regulations as well as privacy policies. For a healthy Cloud Security apart from the outsider's security management inside attacks and risk also need to manage [22], [25].

7. CONCLUSION :

Security is an important concern these days and as far as Information Technology is concerned security is most vital affairs to be noted. Today most of the organizations are employing Information Technology and today among the emerging technologies Cloud Computing is a big name. Cloud model is applicable in different types of organizations and institutions including government organizations and bodies. Moreover, proper policy, regulation, framework designing, development as well as implementation are also important. It is worthy to mention that, for a better security both Cloud Service providers and customers joint initiatives are much important. As today common people are also using huge cloud based products and services so that their minimum knowledge on the field and awareness highly desirable.

REFERENCES:

[1] Aljawarneh, S. A., Alawneh, A., & Jaradat, R. (2017). Cloud security engineering: Early stages of SDLC. *Future Generation Computer Systems*, *74*, 385-392.

[2] Bellavista, P., Corradi, A., & Stefanelli, C. (2001). Mobile agent middleware for mobile computing. *Computer*, *34*(3), 73-81.

[3] Bishop, M. (2003). What is computer security?. *IEEE Security & Privacy*, *1*(1), 67-69.

[4] Bonner, W., & Chiasson, M. (2005). If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. *Information and Organization*, *15*(4), 267-293.

[5] Borgesius, F. Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30*(3), 2073-2131.

[6] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

[7] Che, J., Duan, Y., Zhang, T., & Fan, J. (2011). Study on the security models and strategies of cloud computing. *Procedia Engineering*, *23*, 586-593.

[8] Chou, T. S. (2013). Security threats on cloud computing vulnerabilities. *International Journal of Computer Science & Information Technology*, *5*(3), 79.

[9] George, B., & Valeva, A. (2006, March). A database security course on a shoestring. In *ACM SIGCSE Bulletin* (Vol. 38, No. 1, pp. 7-11). ACM.

[10] Goth, G. (2012). Mobile security issues come to the forefront. *IEEE Internet Computing*, *16*(3), 7-9.

[11] Holla, S., & Katti, M. M. (2012). Android based mobile application development and its security. *International Journal of Computer Trends and Technology*, *3*(3), 486-490.

[12] Jamil, D., & Zaki, H. (2011). Security issues in cloud computing and countermeasures. *International Journal of Engineering Science and Technology (IJEST)*, *3*(4), 2672-2676.

[13] Krishnan, V., McCalley, J. D., Henry, S., & Issad, S. (2011). Efficient database generation for decision tree based power system security assessment. *IEEE Transactions on Power systems*, *26*(4), 2319-2327.

[14] Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN)*, *3*(5), 247-255.

[15] Lee, K. (2012). Security threats in cloud computing environments. *International journal of security and its applications*, *6*(4), 25-32.

[16] Ngai, E. W., & Gunasekaran, A. (2007). A review for mobile commerce research and applications. *Decision support systems*, *43*(1), 3-15.

[17] Nkosi, M. T., & Mekuria, F. (2010). Cloud computing for enhanced mobile health applications. In *2010 IEEE Second International Conference on Cloud Computing Technology and Science* (pp. 629-633). IEEE.

[18] Okuhara, M., Shiozaki, T., & Suzuki, T. (2010). Security architecture for cloud computing. *Fujitsu Sci. Tech. J*, *46*(4), 397-402.

[19] Paul, Prantosh Kumar, Aithal, P. S. and Bhuimali, A. Kalishankar, Tiwary and Rajesh, R., (2019). FIPPS & Information Assurance: The Root and Foundation (June 15, 2019). Proceedings of National Conference on Advances in Management, IT, Education, Social Sciences (MANEGMA 2019), Mangalore. *1*(1) pp. 27-34.

[20] Siau, K., Lim, E. P., & Shen, Z. (2001). Mobile commerce: Promises, challenges and research agenda. *Journal of Database Management (JDM)*, *12*(3), 4-13.

[21] Siau, K., & Shen, Z. (2003). Mobile communications and mobile services. *International Journal of Mobile Communications*, *1*(1-2), 3-14.

[22] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.

[23] Vaquero, L. M., Rodero-Merino, L., & Morán, D. (2011). Locking the sky: a survey on IaaS cloud security. *Computing*, *91*(1), 93-118.

[24] Varshney, U., Vetter, R. J., & Kalakota, R. (2000). Mobile commerce: A new frontier. *Computer*, *33*(10), 32-38.

[25] Welp, Y., Urgell, F., & Aibar, E. (2007). From bureaucratic administration to network administration? An empirical study on e-government focus on Catalonia. *Public Organization Review*, *7*(4), 299-316.

****