Vulnerabilities in Cloud Computing Domain: A Review

Arunkumar Kandru[1], B. Vijaykumar[2], P. Sanjeeva[3]

[1]Assistant Professor, Department of CSE, MREC (A), Hyderabad, Telangana State, India.
[2, 3]Associate Professor, Department of CSE, MREC (A), Hyderabad, Telangana State, India.

Received date: 23rd March, 2017, Revised Date: 2nd May, 2017, Accepted Date: 10th May, 2017

Abstract - "Cloud" is intended to provide a variety of tasks like custom online storage space, development, and deployment of customized software products, adoption of business and related applications, the creation of real-time network environment with full-fledged infrastructure and much more. The main characteristic feature of Cloud Computing is shared support, dynamic provisioning of services, intended network access and monitoring the managed services for optimized access with authentication rights. The objective of this article is to throw the light on security breaches in the Cloud Computing field and recent activities with future research scope in the Cloud Computing domain.

Keywords - Cloud Computing, Threats, Security Challenges, Encryption Algorithms, Cloud Services.

I. INTRODUCTION

Cloud computing provides shared access and storage of data which may be accessed over the internet. Main benefits of cloud services are provisioning of self-service, elasticity and pay for usage methodology. There are many reasons to represent the cloud as a big deal. Among them, few are does not require any maintenance from customer end, unlimited size and anywhere access. Organization of this article is as follows: Section 2 deals with some of the related works related to Cloud Security issues and part 3 focuses on security challenges. Section 4 draws the conclusion and future scope of the security issues in Cloud domain.

II. RELATED WORKS

According to Gagandeep Kaur and Arvinder Kaur [2], there is a security threat to data which is stored in the cloud environment. To protect the data from the unauthorized users, they have enhanced some features to the Cloud Service Access Control. Role-based Access Control and Cloud Service Access Control is the existing access control models. In Cloud Service Access Control before serving the services to the user, first Cloud Service Provider (CSP) checks the service level agreement and then checks for the payment status. If the CSP subscribed for a particular service, then CSP gives access to that service only based on role. The payment situation of the Cloud Service user is checked by the algorithm which is the combination of Rivest, Shamir and Aldeman (RSA) and Advance Encryption Standards (AES). Before giving the access permission to the Cloud Service User (CSU), the CSP has to check whether the CSU is authorized or not by sending the key to the mail of the account holder. The algorithms that generate key are RSA and AES algorithm, respectively. The policy conflict detection algorithm is used to find the conflicts and to reduce the number of conflicts. If any conflict occurs, then those conflicts are assigned to the two roles and those particular functions will be denied. The results of the evaluation show that their access control system has less problem of explosion of concepts than role based access control and cloud service access control. Therefore, their model has less operation cost than role based access control and cloud service access control. However, their system failed to consider The Web Ontology Language (OWL) issues. The problem of deadlock in the web ontology language files system and access permission conflicts were left open for future enhancements.

In 2015, [3] discussed security threats like data leakage or loss in the cloud. To overcome those security issues, the user has to select the best service provider who is providing better security. Security Threat Measurement Model (STMM) was introduced to find service providers security maturity. Before selecting the cloud vendor, the customer has to raise the security issues, such as regulatory compliance, privileged user access, data segregation, data location, recovery, investigative support and login terms. In this method, all the security issues are categorized into six types as, user and privileged user qualifications, security events detection, malicious staff management, continuously improvement mechanism, data loss or leakage and responsibility, security system or certification mechanism. Security threats are categorized into three types, namely system level security, management level safety and technique level security. Using STMM, the user can choose a higher level security cloud service provider or ask the service vendor to improve the security.

Ling-Li Lin Xu Jing Li Changchun Zhang [4] now a day's it is tough to identify who is the trusted Cloud service vendor, it is necessary to know which CSV was providing Trusted services to the Cloud Service User Because on cloud environment CSU is lost their control over their data. So many Cloud Service Vendors are in the present market, so it 's hard to choose one of them. To access the data from the cloud, the user has to be authenticated and authorized. The problems from the side of Cloud Service Providers are authentication errors, hardware failure, and service delays. The CSV who provide reliable services those CSV are got popularity. The Third Party Audit is the third party between Cloud Service user and Cloud Service Provider and TPA is an individual entity which maintains trusted relation with both the parties. In cloud services so many phases are there users may be unaware of those constraints like security management,

abnormal and fault management, etc. So third party-id required to Monitor all these things and take a survey on different cloud service providers and give the information to the Cloud Service users about its survey. This paper proposed a Third Party Audit mechanism into the file sharing system. The internal audit incurs some cost as well we will get the private behavior of process of the service provider by the internal auditing team. In the audit results, operating process of those providers will be exposed. Service providers may not accept the external audit because only for static data Cloud Service Vendors are supporting the auditing. So to support active data auditing [4] the authors introduced (DPDP) dynamic verifiable data possession, in which the correctness of the audit result can be strictly guaranteed. From the author's perspective, to increase the cloud storage service usage, two fundamental things are essential. The accessibility of service supply for the end user including ample storage space is the first one; operation simplicity is the second one. Based on the fundamental things as mentioned above with open source software Eucalyptus they built a service supply platform. It is mainly used for storage service supply to their campus; users, service providers, and the TPA are the three entities of the cloud storage architecture. To know the level of security and reliability of services Third Party Audit, Mechanism is introduced. To The file sharing system, TPA was introduced and analyzed the safety of the scheme. But it has to be tested with larger storage case.

In 2010, Zhidong Shen, Qiang Tong [5] discussed a method by integrating the Trusted Computing Platform into the cloud computing system to build the trusted cloud computing environment. In cloud computing not only confidentiality and security are important but also availability, reliability, integrity, and safety also necessary. For authentication integrity and privacy in the environment of cloud computing, Trusted Computing Platform is used, and it is hardware independent. Encryption and authenticated boot are the two essential services provided by Trusted Computing Platform. What operating system is running on the system is monitor by the verified boot with the help of adding hardware which keeps an audit log of the boot process. The session key(random number) generated by TCP. The important date is encrypted and stored in the system by use of the key generated by Trusted Computing Platform. The challenging task is how to incorporate or integrate the hardware into the cloud computing.

According to Joel Ahmed Mondol et al., in 2011 [1], a new research strategy towards delivering cloud computing security using reconfigurable FPGA has been discussed. In his presentation, four different solutions were proposed for keeping the data secured. To maintain the control over the data in the hands of data owner FPGA device is introduced. FPGA devices are located client side and directly associate with the CSU. And this FPGA prevents the malicious internal CSP to tamper with IAAS and PAAS. The VM layer is invisible to the attacker. Attaching the virtual devices to a physical device is the main problem with virtual technology. Multitude attacks can be prevented by using FPGA device, and these devices are reprogrammable. If any updates and changes occur, they can be downloaded and up-to-date. Trusted platform, data security, user enabled security, and verifiable attestation is the four solutions implemented on hardware. These solutions can be deployed separately or collectively.

Furfaro, Garro and Tundis [6] proposed an independent meta-model called Security as a Service (SecaaS) for securing the Cloud computing domain. This method consists of three phases, namely Security Service Identification, Design Solution Definition and Design Solution Analysis. During the SecaaS modeling process, the identified core concepts were service, policy, security mechanism and category. After determining the security service conceptual model, two security service design solutions (I and II) were derived with different systems and security mechanism to evaluate this approach. Hence, the proposed method resulted in effective identification with integrated security for Cloud services.

According to Qi-Tao Lin, Chang Dong Wang, Jing Pan, Lu Ling and Jian Huang Lai [7], there is a security problem in every cloud applications privacy and information safety. To protect the data in cloud storage and privacy of cloud storage application user [7], proposed a security scheme based on local encryption is the first idea and the second one is cloud interface. Before placing the information on to the cloud server first encrypt the data at local side system and select the CSP who is providing better security. In their proposed system they have used an algorithm which is based on Blowfish algorithm to encrypt the data at clients end. The primary step of this algorithm expands the user's key. The user key may expand or shrink the maximum length key can expand is 400 bits. There are two key extension boxes one is S-boxes and another is P-boxes to produce strong cipher. It generates the sub-keys using P-boxes and S-boxes and the user information is divided into 64-bit blocks and each block is encipher using Blowfish algorithm. Blowfish algorithm is better than AES and DES. The work to do is develop software to encrypt the data at client side and upload it to cloud server.

III. SECURITY CHALLENGES IN CLOUD COMPUTING DOMAIN

The major security issues in the Cloud Computing domain is categorized as (a) Governance, (b) Compliance, (c) Availability, (d) Data Security, (e) Identity and Access Management, (f) DR/BC Planning. Figure 1 shows the security issues in Cloud domains.

Apart from the major security issues, other security issues associated with Cloud Computing are Multi-tenancy, threats about data leakage, Insecure Application Programming Interface (API), Encryption and Key Management.

Fig. 1 Security Challenges in Cloud Computing domains

IV. CONCLUSION

Cloud computing, not only a boon for the modern world with mixed opportunities, has some security challenges to be addressed in the major domains like protecting the data, authentication of the user, disaster, and data breach scenarios. The other issues are least bothered and need addressing includes week identity and access management, Insecure Application Programming Interfaces (APIs), hijacking the accounts, data loss, denial of service(s), advanced persistent threats, shared technical issues and much more. Even though we are utilizing the benefits of cloud computing and enjoying, a lot of security vulnerabilities in the cloud domain remains unaddressed. Authors would like to work and explore more on the safety risks and make necessary countermeasures to the Cloud security breaches.

REFERENCES

[1] Joel Ahmed and M. Mondol, "Cloud security solutions using FGPA", IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, doi:10.1109/PACRIM.2011.6032987, 2011.

[2] Gagandeep Kaur, Arvinder Kaur, "A Key based Security Mechanism for Payment Status in Cloud Service Access Control System", ICACCI, doi:10.1109/ICACCI.2015.7275685, 2015.

[3] Qi-Tao Lin, Chang-Dong Wang, Jing Pan, Lu Ling and Jian-Huang Lai Local, "Data Security and Privacy Protection in Cloud Service Applications", 9th International Conference on Frontier of Computer Science and Technology, doi:10.1109/ICCSEE.2012.193, 2015.

[4] Ling Li Lin Xu Jing Li Changchun Zhang , "Study on the Third-party Audit in Cloud Storage Service", International Conference on Cloud and Service Computing, doi:10.1109/CSC.2011.6138525, 2011.

[5] Zhidong Shen, Qiang Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology", 2nd International Conference on Signal Processing Systems, IEEE, doi:10.1109/ICSPS.2010.5555234, 2010.

[6] Angelo Furfaro, Alfredo Garro and Andrea Tundis, "Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing", International Carnahan Conference on Security Technology, IEEE, doi:10.1109/CCST.2014.6986995, 2014.

[7] Qi-Tao Lin, Chang Dong Wang,Jing Pan ,Lu Ling and Jian Huang Lai, "Local Data Security and Privacy Protection in Cloud Service Application", Ninth International Conference on Frontier of Computer Science and Technology, IEEE, doi:10.1109/FCST.2015.39, 2015.