International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

A Survey on Security Mechanisms and its Consequences in Cloud Computing

Manjushree.C.V[1], Dr. A. N. Nandakumar[2]
Assistant Professor & Research Scholar, CSE Dept.,
Vemana Institute of Technology, Bangalore, India[1]
Professor, New Horizon College of Engineering, Bangalore, India [2]

Abstract: ***IT modernization and new digital business areas made organizations to move their data to the cloud providers. Services provided by the cloud providers can be accessed through internet. Cloud providers allow organizations to pay as per use basis, they provide on demand services to their customers, load balancing and many security benefits such as centralized data, reduced data loss, monitoring, instant swap over, logging, secure builds, improved software security and security testing. In spite of all this organizations are afraid about their data compromise. In this paper we are going to discuss about a survey on different security mechanisms and their consequences.***

Keywords: ***cloud computing, security, AWS, SSH, REST.***

I. INTRODUCTION

"Cloud computing is a construct that allows you to access applications that actually reside at a location other than your computer". Using cloud computing IT department can focus on their strategic projects instead of maintaining their own datacenter by this operational and capital cost can be reduced. Beauty and the components of cloud computing are shown in the Fig 1 and Fig 2. Even though it is having many benefits cloud computing may not be appropriate for variety of reasons such as legislative issues, geopolitical concerns, when an application is hardware dependent, when an application requires control on amount of memory, CPU, hard drives, cloud bursting, data compromise, data in cloud are stored geographically different locations due to this latency may be a problem, and reliability should be considered when we are running an high speed application in house. Pay as per use is one of the characteristics of cloud computing but when we deploy an application it requires lot of throughput so cost will also be increased. Other than all this issues security is a major risk when we move our data to the cloud environment. In this paper we are going to discuss different mechanisms used in cloud security and their consequences.

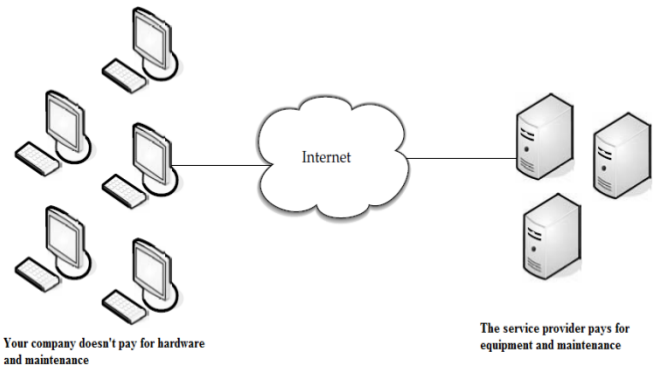

Fig 1. Cloud Computing

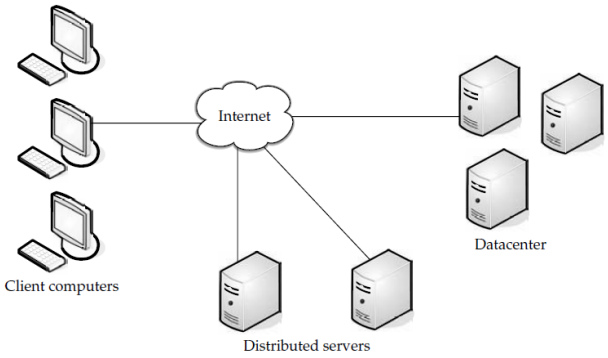

Fig 2: Components of Cloud Computing

II. RELATED WORK

Cloud computing offers different types of services to their customers. Here service is a concept of being able to use reusable, fine grained components across provider's network. Different types of services provided by cloud are shown in Fig 3.

1. Software as a service

In this model hosted applications can be accessed via the internet. Customers who need high powered applications are benefited by this model. Some of the applications provided in this model are video conferencing, customer resource management, accounting, IT service management, web analytics, web content management and some of the benefits of this model are customization, web reliability, security and better marketing. Due to increase in bandwidth and quality of services allow the client to trust that they can access their applications with low latency and good speed. Other than all this benefits and application SAAS is facing many obstacles such as lock in with vendors, availability of open source application, cheaper hardware and organizations will not be able to find application available in SAAS for a specific computational need. Security obstacles in this SAAS model are locality of data, data privacy, and access control on data, data isolation and integrity, sniffing of data on internet, security for web applications, identity management, availability, backup, authentication, and authorization [1].

2. Platform as a service

This model provides a framework to build applications and services from internet. Services provided by PASS are design, development, testing, deployment, hosting of applications, team collaboration, web service integration, database integration, security, scalability, state management, versioning, automatic concurrency management, and failovers. Other than all this benefits PAAS is facing many obstacles such as lock-in with vendors, costs are high for moving applications between conventional host and security obstacles in this model are rapid change of application will affect system development life cycle, disaster recovery and security in development tools. PAAS are often used in conjunction with other applications known as mashup hence we need to consider issues related to mashup such as network and data security [1].

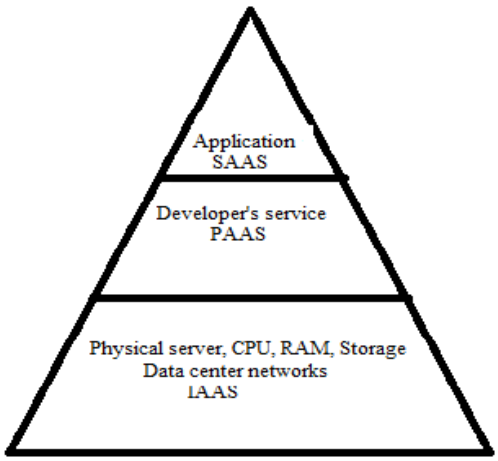

Fig 3. Cloud computing services.

3. *Hardware as a service*

In this model vendor's provide hardware resources. Organization can put whatever they want onto it. Hardware resources given by providers for rent are server space, network equipment, memory, CPU cycles, and storage space. Some of the benefits provided by this model are dynamic scale up and scale down of infrastructure, multiple tenants can be equipped at same time, billing is based on utility computing, platform virtualization environment, and SLA are signed between providers and client to guarantee the level of performance. Other than all this benefits IAAS is facing many security obstacles such as weak SLA, attacks on virtualization, malicious virtual machine monitors are able to monitor the resources in multi tent environment and security management in lifecycle of virtual machines [1].

III. CURRENT SECURITY MECHANISMS AND CHALLENGES

1. *S2N*

It is a security tool used in amazon web services (AWS) and a new implementation of TLS encryption protocol former openSSL. TLS protocol provides privacy and integrity between two communicating protocol applications. In this protocol private connection is established by using symmetric cryptography to encrypt the data. Integrity is achieved by message integrity check of using message authentication. But there are many significant vulnerability attacks on this TLS protocol. One of such attack is lucky 13 cryptographic timing attacks on s2n security tool. To overcome this attack amazon cloud providers have included solutions one by minimizing the timing difference and other by including delay of up to 10 seconds whenever errors are triggered. Even though there are many challenges for protecting the data against sophisticated timing attacks and standard code audits are insufficient to uncover all cryptographic attack vector.

2. *Threshold cryptography*

In this method data is encrypted using public key and private key is shared among participating users. Cooperation of several parties are required for decryption of the message. One of the new method that was introduced was using of capability list to control the data access. Using this capability list we can store the information about user and their access rights to data. But they are lacked in some ways such as violation of data privacy because of collision attack and heavy computation. To overcome this attack single key was given for the group to perform encryption and decryption. Threshold cryptography is an excellent mechanism for evoting, group authentication, key sharing and techniques of digital signature. But still for the wide adoption and successful implementation of threshold cryptographic scheme standardization is required in this area.

3. *Log files analysis method*

Log file contains a data generated from different transactions when we are navigating from one web site or application to another. Log contains information about user identifiers, system identifiers, operation done and time. Using this log files detecting of attacks will be easier. But one of the challenge in this area is volume and high scale variety in which logs are produced, recorded, data is structured, decentralization. To overcome this drawback log files are centralized. For centralization many data mining techniques were used like FP growth approach to prevent attacks. But in this approach there are many shortcomings such as fail of central computer, quality of administration and availability of resources. All these obstacles need to be overcome in this method.

4. *SSH(secure socket shell)*

It is a cryptographic network protocol that provides authentication and encryption between two computers when it is connected through internet. SSH are mainly used by network administrator for managing system resources and applications remotely and they also allow for remote login, movement of files from one computer to another, remote execution access to shell accounts on Unix like operating systems. In spite of all these advantages threats are poor key management, attacks on API key, user credentials, publisher credentials and if centralization is not done properly, rotation and removal of SSH keys organization can lose access control on customer data.

5. *REST(Representational state transfer)*

It is a data communication mechanism that establishes interoperability between client and cloud providers by using HTTP protocol. In REST every component is a resource and these resources are accessed by using standard HTTP methods. Benefits offered by Restful API are use of hyperlinks in representation, better response time, reduced server load, less client side soft wares need to be written because single browser can access any application and any resource, and long term compatibility and evolving characteristics. To provide security cloud providers need to control the access to the interface through policy enforcement. Limitations to the policy enforcement are there are no uniform standards regarding policy language and for the implementation of policy enforcement users have to deal with certain types of policies to accommodate certain system, platform specific authorization policy language and related mechanisms need to be designed by cloud providers. To overcome this limitations RESTPL (Request oriented access control language) was designed but enforcement overhead was reduced only by 80%.

6. Color scheme for data protection

It is implemented on private cloud. It is a two-step authentication process. For registration user has to follow the following steps. In first step user has to give first name, last name, userid and contact number. In the second step user has to select randomly on any three colors and shades (white, gray and black) both the colors and shades need to be memorized. For authentication process user has to specify username and sequence of shades. If they are incorrect then authentication process will terminate. In the second step of authentication user has to select the number displayed on color in color grid, it represent column number. Row is identified as per the sequence of shade chosen at the time of registration. Then user has to select three digit number available in numeral grid by using identified row and column concatenate three digit number retrieved from numeral grid to get one time password box repeat this step for selected colors. In this research security for generating password was achieved but generating of random alphanumeric and special characters need to be improved.

7. Access control mechanisms in cloud

One of the method used for controlling data access in cloud computing is attribute based encryption. In this method of access control many research has been taken place due to its challenges such as non-efficiency, non-existence, key coordination, key escrow and key revocation. Methods of attribute based encryption available to overcome this challenges are CP-ABE, key policy attribute encryption. Using this two methods data owner can place fine grained and cryptographically enforced access control over outsourced data. But security issues in this area such as user revocation, backward and forward security are reduced little but still not completely eliminated.

8. Bio inspired model to provide data security in cloud

Bio inspired model is an amalgamation of genetic algorithm and attribute based encryption. It is capable of processing complex information and providing solutions to many problems. In this model genetic algorithm is used to encrypt the data before sending it to the cloud and attribute based encryption is used for key generation and management. Using this model latency is decreased and performance is increased but only single user can encrypt the data before sending it to the cloud and decrypt the data after downloading from the cloud it cannot be used for data sharing between multiple users.

IV. CONCLUSION AND FUTURE WORK

The ever evolving field of Computer Science in general and Cloud Computing in specific has been throwing up new opportunities and challenges equally. One of the key aspects in Cloud Computing being sharing of resources among many tenants security has evidently emerged as a concern while the world is celebrating the evolution of cloud and all its related tools and technologies along with its best practices . There is no doubt that security aspects are still a daemon running at every cloud scientist mind. The latest and the greatest technologies have realized the true usage of cloud and its resources. Containerization being the new kid on board has caught attention among large enterprises for its ease of development, deployment and promotion. Further research and development work would focus on this with security driven research.

REFERENCES

[1]. Keshmasuryawanshi, Santosh shelke, improving data storage security in cloud environment using public auditing and threshold cryptography scheme, proceedings of International Conference on Computing Communication Control and automation (ICCUBEA), 2016
[2]. Syed Asad Hussain, Mehwish Fatima, Atifsaeed, Imran Raza, Raja KhurranShahzad," Multilevel classification of security concerns in cloud computing", applied computing and informatics, vol.13, issue1january 2017, pages 57-55
[3]. Martin R., Albrecht and Kenneth.G.paterson., A timing attack on amazon S2N implementation of TLS, Eurocrypt1, pp 622-643, 2016
[4]. Yang Luo, Hongbo Chou, Qingnishen, AnbangRuan, Zhonghai Wu, RestPL: towards a request oriented policy language for arbitrary Restful API, proceedings of International Conference on web services(ICWS),2016
[5]. ShimpyHarbajanka, PreetiSaxena, survey paper on trust management and security issues in cloud computing, Symposium on Colossal Data Analysis and Networking (CDAN), 2016
[6]. Mohammed UbaidullahBokhari, QahtanmakkishallaiyahyakordTamandani., cloud computing service models: A comparative study, proceedings of 3rd International Conference on Computing for Sustainable Global Development(INDIACom), 2016
[7]. Weiwei Kong, Yang Lei, Jing Ma, data security and privacy information challenges in cloud computing, proceedings of International Conference on Intelligent Networking and Collaborative Systems, 2016
[8]. Meryem Amar, MouadLemoudden, Bouabidel Ouahindi, Log file centralization to improve cloud security, proceedings of 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), 2016
[9]. Irina Astrova, Arne Koschel, Mats Lennart Henke, IaaS platforms: How Secure are They?, proceedings of International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2016

