© 2018 IJSRST | Volume 4 | Issue 11 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : https://doi.org/10.32628/IJSRST18401110

A Case Study : Security as A Service (SAAS) in Cloud Computing Environment

Vivekanand[1], Trilok Singh Randhawa[2]

[1](CEH, COBIT5, ASM, DevOps Master, ISO IEC 27001, AWS-SAA, Prince2 Practitioner, ITIL, RHCE), Member of OCEG GRC and Block chain Council, India

[2]PhD Researcher, Department of Management Studies, Sarvepalli Radhakrishnan University, Bhopal, India

ABSTRACT

Security-as-a-service (SaaS) is an outsourcing model for security management in cloud computing environment. The researcher focused on the some of the significant research issues in cloud computing typically, Security as a Service involves applications on AMAZON online shopping portal and its controlling mechanism in cloud computing environment. Outsourcing of administrative tasks, such as log management, to save time and money and allow an organization to devote more time to its core competencies. A Web interface that allows in-house administration of some tasks as well as a view of the security environment and on-going activities. The researcher proposed a model as applied to information security type services and does not require on-premises hardware, avoiding substantial capital outlays. These security services often include authentication, anti-virus, anti-malware/spyware, intrusion detection, and Penetration testing and security event management, among others.

Keywords : SaaS, IT, IDC, Cloud Computing

I. INTRODUCTION

Cloud computing is the most envisioned paradigm shift in computing world. Its services are these days generally being applied in several IT scenarios. Cloud computing is a recently developed technology for complex systems with large-scale services sharing among multiple users. Therefore, authentication and integration of both users and services is a significant issue for the trust and security of the cloud computing unique platform has brought new security issues to contemplate. Cloud computing is essentially the management and provision of applications, information and data as a service. These services are provided over the internet, often on a pay-as-you-go based model. Cloud computing provides a convenient way of accessing computing services, independent of the hardware you use or your physical location. It relieves the need to store information on your PC, mobile device or gadget with the assumption that the information can be quickly and easily accessed via the net. Cloud computing provides clients with a virtual computing infrastructure which enables them to store data and run applications. Cloud computing introduces new security challenges as client can't fully trust cloud providers. Cryptography in cloud computing depends on a secure cloud computing architecture. Cloud computing is a computing model that is driven by economies of scale and is distributed on large scale. Cloud architectures are developed according to latest and urgent demands. That is, the resources are dynamically provided to a user as per his request, and taken back after the job is done. Cloud computing is a service pool which includes the hardware and operating system infrastructure, the formation of systems management software, system and platform, and virtualization components.

Security has always been the main issue for IT Executives when it comes to cloud computing and its adaptation. In two surveys carried out by IDC in 2008 and 2009 consecutive years security topped the list. However, cloud computing is aggregation of technologies, operating systems, storage, networking, virtualization, each fraught with inherent security issues. For example, browser based attacks, denial of service attacks and network intrusion became carry over risks into cloud computing world. The benefits of using cloud computing are very well known and several of the benefits are outlined above. However, cloud computing is not without its pitfalls. The majority of which center around security of data that is stored in the cloud. There are potentials for a new wave of large- scale attacks via the virtualization platform. Cattedu et al. (2009) described the "Fear of the Cloud" by categorizing security concerns into three traditional concerns, availability and third party data control.

Clouds bring out tremendous benefits for both individuals and enterprises. Clouds support economic savings, outsourcing mechanisms, resource sharing, any-where any-time accessibility, on-demand scalability, and service flexibility. Clouds minimize the need for user involvement by masking technical details such as software upgrades, licenses, and maintenance from its customers. Clouds could also offer better security advantages over individual server deployments. Since a cloud aggregates resources, cloud providers charter expert security personnel while typical companies could be limited with a network administrator who might not be well versed in cyber security issues. Similarly, clouds are more resilient to Distributed Denial of Service (DDoS) attacks due to the availability of resources and the elasticity of the architecture. The clouds support mobile computations where Virtual Machines (VMs) migrate from one physical machine to another's M. Khalil and Abdullah Khreishah (2014).

II. BACKGROUND OF RESEARCH STUDY

C. Linda Hepsiba and J.G.R.Sathiaseelan (2016) stated that the cloud computing is an emerging technology for providing computing resources and storage to all kinds of users. This technology is facing lot of challenges including data and network security, interoperability, legal and compliance issues. In security issues, there exist numerous risks for the data processed or stored in the cloud environment. Cloud data are may be used by unauthorized access or users. This paper is mainly focused on security issues for cloud service models like and their solutions.

Md. Sakib Bin Alam (2017) focused on the cloud computing system delivers computing resources as a service over the network. During the last few years clod computing technology has gained attention due to its autonomous and cost effective services. It is responsible for the growth of IT industry. But cloud computing has various security challenges that hinder the rapid adoption of this computing paradigm. Efficient steps should be taken to make cloud computing more secure and reliable. This paper works on overview of clod computing as well as related security issues.

Hassan TakabiAndjamesB.D.Joshi (2010) emphasized on cloud computing has generated significant interest in both academia and industry, but it's still an evolving paradigm. Essentially, it aims to consolidate the economic utility model with the evolutionary development of many existing approaches and computing technologies, including distributed services, applications, and information infrastructures consisting of pools of computers, networks, and storage resources. Confusion exists in IT communities about how a cloud differs from existing models and how these differences affect its adoption. Some see a cloud as a novel technical revolution, while others consider it a natural evolution of technology, economy, and culture.

Deshmukh et al. (2015) discussed as the data produced by the enterprises that need to be stored and utilized (e.g. emails, personal health records, photo albums, tax documents, financial transactions, etc.) is rapidly increasing, data owners are motivated to outsource their local complex data management systems into the cloud for its great flexibility and economic savings. Cloud storage allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. In cloud storage, the data will be stored in storage provided by cloud service provider (CSP's). Cloud service providers must have a viable way to protect their client's data, especially the data from disclosure to unauthorized users. But in data privacy protection and data retrieval control is most challenging research work in cloud computing. Also service provider must provide authentication for valid user otherwise security reduce and cloud system may collapse.

Pradeep Kumar Tiwari and Dr. Bharat Mishra (2012) focused on the cloud computing is an Internet-based computing, where shared resources, software and information, are provided to computers and devices on-demand. It provides people the way to share distributed resources and services that belong to different organization. Since cloud computing uses distributed resources in open environment, thus it is important to provide the security and trust to share the data for developing cloud computing applications. In this paper we show Successful implementation of cloud computing in an enterprise requires proper planning and understanding of emerging risks, threats and possible countermeasures. This paper show how we secure the cloud security, privacy and reliability when a third party is processing sensitive data. In this paper, we have discussed security risks and concerns in cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources.

Muhammad Faheem Mushtaq and UroojAkram (2017) focused on the cloud computing exhibits a remarkable potential to offer cost-effective and more flexible services on-demand to the customers over the network. It dynamically increases the capabilities of the organization without training new people, investment in new infrastructure or licensing new software. Cloud computing has grown dramatically in the last few years due to the scalability of resources and appear as a fast-growing segment of the IT industry. The dynamic and scalable nature of cloud computing creates security challenges in their management by examining policy failure or malicious activity. In this paper, we examine the detailed design of cloud computing architecture in which deployment models, service models, cloud components, and cloud security are explored. Furthermore, this study identifies the security challenges in cloud computing during the transfer of data into the cloud and provides a viable solution to address the potential threats.

R. VelumadhavaRaoa and K. Selvamanib(2015) emphasized on cloud Computing trend is rapidly increasing that has an technology connection with Grid Computing, Utility Computing, Distributed Computing. Cloud service providers such as Amazon IBM, Google's Application, Microsoft Azure etc., provide the users in developing applications in cloud environment and to access them from anywhere. Cloud data are stored and accessed in remote server with the help of services provided by cloud service providers. Providing security is a major concern as the data is transmitted to the remote server over a channel (internet). Before implementing Cloud Computing in an organization, security challenges needs to be addressed first. In this paper, we highlight data related security challenges in cloud based environment and solutions to overcome.

Issa M. Khalil and Abdullah Khreishah (2014) focused on cloud computing is an emerging technology paradigm that migrates current technological and computing concepts into utility-like solutions similar to electricity and water systems. Clouds bring out a wide range of benefits including configurable computing resources, economic savings, and service flexibility. However, security and privacy concerns are shown to be the primary obstacles to a wide adoption of clouds. The new concepts that clouds introduce, such as multi-tenancy, resource sharing and outsourcing, create new challenges to the security community. Addressing these challenges requires, in addition tithe ability to cultivate and tune the security measures developed for traditional computing systems, proposing new security policies, models, and protocols to address the unique cloud security challenges.

Rabi Prasad Padhy and ManasRanjan Patra(2011) emphasized that cloud computing is an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc.

III. PROBLEM STATEMENT

The cloud computing is a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies and it has more advantage characters such as large scale computation and data storage, virtualization, high expansibility, high reliability and low price service. The security problem of cloud computing is very important and it can prevent the rapid development of cloud computing.

IV. RESEARCH OBJECTIVES

This paper introduces some cloud computing systems and analyses cloud computing security problem and its strategy according to the cloud computing concepts and characters. The data privacy and service availability in cloud computing are the key security problem. Single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system. The researcher stated the some of the significant research issues with respect to analysis of cyber security solution: security as services (SaaS) in cloud computing environment.

1. What are the affecting factors responsible for cyber security in cloud computing environment?
2. What are the solution attributes to protect and analyze the cyber security issues in cloud computing?

CONCEPTUAL FRAMEWORK OF THE RESEARCH STUDY

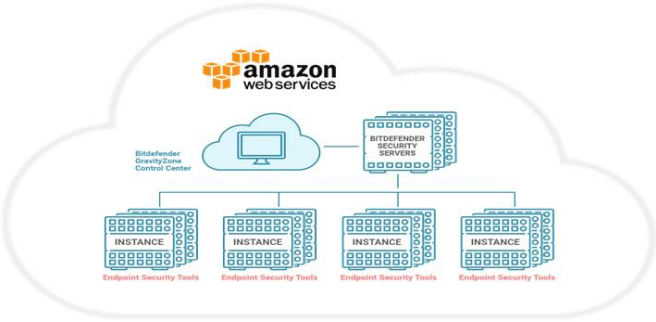

Fig 1. Framework of the Security as a Service in Cloud Computing Environment

CASE STUDY: SECURRITY AS SOLUTION

Recent advances have witnessed the success and popularity of cloud computing, which represents a new business model and computing paradigm. The feature of on-demand provisioning of computational, storage, and bandwidth resources has driven modern businesses into cloud services. The cloud is considered cutting edge technology and it is solely relied on by many large technology, business, and media companies such as Netflix or Salesforce.com. However, in addition to the benefit at hand, security issues have been a long-term concern for cloud computing and are the main barriers of the widespread use of cloud computing. In this paper, we briefly describe some basic security concerns that are of particular interest to cloud technology. We investigate some of the basic cloud concepts and discuss cloud security issues. Amazon Web Services is used as a case study for discussing common cloud terminology. Data security, as well as some cloud specific at-tacks is introduced. In this paper, we provide an overview of cloud security in various aspects. We first review the data storage scheme for Amazon's cloud. The unique forms of products and services offered through cloud services show the incentive for modern business use. Using Amazon Web Services as a case study, we are able to implore some of the basic terms and concepts of cloud computing. We then proceed to discuss data security, API concerns, account hijacking, and other security concerns.

These general concerns are shown to be of particular interest to cloud security. The main differences between traditional services and cloud services are compared from a security perspective. Service and account hijacking is covered, as well as possible defenses. It is found the differences between security issues in cloud services and in traditional services, the researcher briefly overview the security in cloud. The study in this paper provides a guideline of research on cloud services and security issues. Finally, we give some ideas on how to build a more secure cloud. Our future work will focus on the security concerns in cloud services. It will include the privacy protection of data information stored in cloud, data integrity with multiple backups for services purpose, etc.

V. CONCLUSION

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. The researcher presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. Storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of

virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines.

VI. RESEARCH ISSUES ON SECURITY

Attackers over the past three years have begun to actively target the digital keys used to secure the Internet infrastructure. Stuxnet's creators stole code-signing keys and then used them to allow the malware to more easily evade host-based security. An alleged Iranian hacker broke into a partner of registry Comodo and bought Secure Sockets Layer (SSL) keys for major domains to eavesdrop on activists. And unknown attackers stole important information on RSA's Secure ID token, a device that generates one-time keys to strengthen online security.

The unique codes that applications in the cloud use to identify one another could be next, security experts say. So-called API keys are used by Web and cloud services to identify third-party applications using the services. If service providers are not careful, an attacker with access to the key can cause a denial-of-service or rack up fees on behalf of the victim.

"It was created as a fairly no authoritative identifier -- it was only there to identify applications or the application's use of an API," says K. Scott Morrison, chief technology officer of Layer7 Technologies, a provider of Web security and governance products. "The problem is that developers have started using API keys for stuff that matters."

The problem is not any inherent weakness in the keys, but that developers use them for security when they ought not, he says. In many implementations, the keys are used to identify users, even though the technology was not meant as a way to authorize access to data. And after expanding the power of the keys, developers do not treat them as critical assets. Instead, companies fail to keep track of the keys, e-mailing them around and storing them on desktop hard drives.

VII. REFERENCES

[1]. C. Linda Hepsiba and J.G.R.Sathiaseelan (),' Security Issues in Service Models of Cloud Computing', International Journal of Computer Science and Mobile Computing, Vol.5 Issue.3, March- 2016, pg. 610-615, ISSN 2320-088X.

[2]. Md. Sakib Bin Alam (2017),'Cloud Computing - Architecture, Platform and Security Issues: A Survey', Department of Computer Science and Engineering, Faculty of Science and Engineering, International Islamic University Chittagong, Chittagong - 4318, Bangladesh World Scientific News 86(3) (2017) 253-264,EISSN 2392-2192

[3]. Hassan TakabiAndjamesB.D.Joshi(2010),' Security And Privacy Challenges In Cloud Computing Environments', Co-published By The IEEE Computer And Reliability Societies, 1540-7993/10/$26.00 © 2010 IEEE., November/December 2010

[4]. Deshmukh et al.(2015),'Security on Cloud Using Cryptography', International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015 ISSN: 2277 128X

[5]. Catteddu, D. and Hagen, G (2009),'Cloud Computing: benefits, risks and recommendations for information security', Technical Report-European Network and Information Security Agency, 2009.

[6]. Pradeep Kumar Tiwari and Dr. Bharat Mishra(2012),'Cloud Computing Security Issues, Challenges and Solution', International Journal of Emerging Technology and Advanced Engineering,ISSN 2250-2459, Volume 2, Issue 8, August 2012)

[7]. Muhammad Faheem Mushtaq and UroojAkram(2017),' Cloud Computing Environment and Security Challenges: A Review', (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 8, No. 10, 2017

[8]. R. VelumadhavaRaoa and K. Selvamanib (2015),'Data Security Challenges and It's Solutions in Cloud Computing', International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) Procedia Computer Science 48 (2015) 204 - 209.

[9]. Issa M. Khalil and Abdullah Khreishah (2014),'Cloud Computing Security: A Survey', computers ISSN 2073-431X, Received: 5 September 2013; in revised form: 14 November 2013 / Accepted: 27 January 2014 / Published: 3 February 2014.

[10]. Rabi Prasad Padhy and ManasRanjan Patra(2011),'Cloud Computing: Security Issues and Research Challenges',IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011,ISSN: 2249-9555.

[11]. WentaoLiu (2012),'Research on cloud computing security problem and strategy', Published in: 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet) IEEE Xplore: 17 May 2012.

DETAILS ABOUT THE AUTHOR

VIVEKANAND

(CEH, COBIT5, ASM, DevOps Master, ISO IEC 27001, AWS-SAA, Prince2, Practitioner, ITIL, RHCE) is a Member of OCEG GRC and Block chain Council. He working on Cyber Security, penetration testing, incident handling, and intrusion detection services, IS Compliance at Flex Trade Systems. Vivek'a has started his career in 2006 as a Unix/Linux administrator for a WIPRO InfoTech company. He gained information security experience in a variety of industries, including banking, insurance, hotel, telecom, power, Internet, and Finance, in positions ranging from systems administrator to Database/Developer to SI Lead and SaaS Lead. He has involved in various key projects related to security and Software as a Services.

TRILOK SINGH RANDHAWA

PhD Research Scholar, Department of Management Studies, Sarvepalli Radhakrishnan University, Bhopal, India