© 2019 IJSRST | Volume 6 | Issue 4 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : 10.32628/IJSRST196492

Analysis of Cyber Security Solution: Security as a Services (SaaS) in Cloud Computing Environment

Dr. Bechoo Lal[1], Dr. Chandrahauns R Chavan[2]

[1]Assistant Professor, Department of Information Technology, Western College, University of Mumbai, India

[2]Professor and Former Director, JBIMS, University of Mumbai, Mumbai, India

ABSTRACT

The researcher emphasized that 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 environment on cyber security. The Security as a Service (SaaS) involves applications such as anti-virus software, system securing attributes which are delivered over the internet on payment basis and services will be taken back once the contract are finished or terminated by the terms and conditions. The controlling mechanism of constant virus updates that are not reliant on user compliance. Greater security expertise that is typically available within an organization. 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 cloud model as applied to information security type services and does not require on-premises hardware, avoiding substantial capital outlays. These security as a services often include authentication, anti-virus, anti-malware/spyware, intrusion detection, and penetration testing and security event management, and among others phases in cloud computing environment. The researcher also emphasized that two real life case study on security as services in cloud computing environment and representing a statistical analysis report which is based on challenges of using cloud computing worldwide as of 2018.

Keywords : SaaS, IT, IDC, Cloud Computing

I. INTRODUCTION

The researcher emphasized that cloud computing is computing services which are providing on demand and payment basis wherever is required and the organizations are taken back their services once the requirements are full-filled or contracts are finished. The most unreal paradigm shift in computing world. Its services are nowadays usually being applied in many IT situations. Cloud computing could be a recently developed technology for advanced systems with large-scale services sharing among multiple users. Therefore, authentication and integration of each users and services could be an important issue for the trust and security of the cloud computing distinctive platform has brought new security problems to ponder[1]. Cloud computing is basically the management and provision of applications, info and information as a service. These services are provided over the web, usually on a pay-as-you-go primarily based model. Cloud computing provides a convenient approach of accessing computing services, freelance of the hardware you employ or your physical location [2]. It relieves the requirement to store info on your computer, mobile device or widget with the idea that the knowledge will be quickly and simply accessed via the online.

Cloud computing provides shoppers with a virtual computing infrastructure that permits them to store information and run applications. Cloud computing introduces new security challenges as consumer can't totally trust cloud suppliers. Cryptography in cloud computing depends on a secure cloud computing design. Cloud computing could be a computing model that's driven by economies of scale and is distributed on giant scale. Cloud architectures are developed per latest and imperative demands. That is, the resources are dynamically provided to a user as per his request, and brought back once the duty is completed. Cloud computing could be a service pool which incorporates the hardware and software package infrastructure, the formation of systems management software package, system and platform, and virtualization parts[3][4].

Security has perpetually been the most issue for IT Executives once it involves cloud computing and its adaptation. In 2 surveys administrated by IDC in 2008 and 2009 consecutive year's security topped the list. However, cloud computing is aggregation of technologies, operational systems, storage, networking, virtualization, every fraught with inherent security problems. As an example, browser primarily based attacks, denial of service attacks and network intrusion became carry over risks into cloud computing world. The advantages of victimization cloud computing are o.k. acknowledged and a number of other of the advantages are made public higher than. However, cloud computing isn't while not its pitfalls. The bulk of that focus on security of information that's keep within the cloud [5]. There are potentials for a brand new wave of large- scale attacks via the virtualization platform. Cattedu et al. (2009) delineate the "Fear of the Cloud" by categorizing security issues into 3 ancient issues, convenience and third party information management [6].

Clouds bring out tremendous edges for each people and enterprises. Clouds support economic savings, outsourcing mechanisms, resource sharing, any-where any-time accessibility, on-demand measurability, and repair flexibility. Clouds minimize the requirement for user involvement by masking technical details like software package upgrades, licenses, and maintenance from its customers. Clouds might additionally provide higher security benefits over individual server deployments. Since a cloud aggregates resources, cloud suppliers charter skilled security personnel whereas typical firms may well be restricted with a network administrator UN agency won't be versed in cyber security problems. Similarly, clouds are a lot of resilient to Distributed Denial of Service (DDoS) attacks because of the supply of resources and also the snap of the design. The clouds support mobile computations wherever Virtual Machines (VMs) migrate from one physical machine to a different Issa M. Khalil and Abdullah Khreishah (2014)[7][8].

II. BACKGROUND OF RESEARCH STUDY

C Linda Hepsiba and J.G.R.Sathiaseelan (2016) expressed that the cloud computing is associate rising technology for providing computing resources and storage to all or any styles of users. This technology is facing ton of challenges together with knowledge and network security, ability, legal and compliance problems. In security problems, there exist varied risks for the information processed or keep within the cloud setting. Cloud knowledge are is also employed by unauthorized access or users. This paper is principally targeted on security problems for cloud service models like and their solutions [1].

Md Sakib Bin Alam (2017) emphasized on the cloud ADPS delivers computing resources as a service over the network. Throughout the previous couple of

years clod computing technology has gained attention thanks to its autonomous and value effective services. It's liable for the expansion of IT business. However cloud computing has varied security challenges that hinder the fast adoption of this computing paradigm. Economical steps ought to be taken to create cloud computing safer and reliable. This paper works on summary of clod computing similarly as connected security problems. [2].

Hassan Takabi and James B.D.Joshi (2010) emphasized on cloud computing has generated important interest in each domain and business, however it's still associate evolving paradigm. Basically, it aims to consolidate the economic utility model with the organic process development of the many existing approaches and computing technologies, together with distributed services, applications, and data infrastructures consisting of pools of computers, networks, and storage resources. Confusion exists in IT communities regarding however a cloud differs from existing models and the way these variations have an effect on its adoption. Some see a cloud as a unique technical revolution, whereas others think about it a natural evolution of technology, economy, and culture [3].

Deshmukh et al.(2015) focused on the knowledge made by the enterprises that require to be keep and used (e.g. emails, personal health records, ikon albums, tax documents, money transactions, etc.) is chop-chop increasing, knowledge homeowners are motivated to source their native complicated knowledge management systems into the cloud for its nice flexibility and economic savings. Cloud storage permits customers and businesses to use applications while not installation and access their personal files at any laptop with web access. In cloud storage, the information are going to be keep in storage provided by cloud service supplier (CSP's). Cloud service suppliers should have a viable thanks to defend their client's knowledge, particularly the information from revealing to unauthorized users. However in knowledge privacy protection and knowledge retrieval management is most difficult analysis add cloud computing. Additionally service supplier should give authentication for valid user otherwise security cut back and cloud system could collapse [4].

Pradeep Kumar Tiwari and Dr. India Mishra (2012) focused on the cloud computing is associate Internet-based computing, wherever shared resources, code and data, are provided to computers and devices on-demand. It provides individuals the thanks to share distributed resources and services that belong to completely different organization. Since cloud computing uses distributed resources in open setting, therefore it's vital to produce the protection and trust to share the information for developing cloud computing applications. during this paper we have a tendency to show undefeated implementation of cloud computing in associate enterprise needs correct coming up with and understanding of rising risks, threats and potential countermeasures. This research article shows a tendency to secure the cloud security, privacy and dependability once a 3rd party is process sensitive knowledge. During this paper, we've got mentioned security risks associated considerations in cloud computing and enlightened steps that an enterprise will want cut back security risks and defend their resources [5].

Muhammad Faheem Mushtaq and Urooj Akram (2017) emphasized that cloud computing exhibits a stimulating potential to supply efficient and a lot of versatile services on-demand to the shoppers over the network. It dynamically will increase the capabilities of the organization while not coaching new individuals, investment in new infrastructure or licensing new code. Cloud computing has mature

dramatically within the previous couple of years thanks to the measurability of resources and seem as an invasive phase of the IT business. The dynamic and scalable nature of cloud computing creates security challenges in their management by examining policy failure or malicious activity. This research study identifies the protection challenges in cloud computing throughout the transfer of knowledge into the cloud and provides a viable answer to handle the potential threats [6].

R Velumadhava Raoa and K. Selvamanib(2015) emphasized on cloud Computing trend is chop-chop increasing that has associate technology reference to Grid Computing, Utility Computing, Distributed Computing. Cloud service suppliers like Amazon IBM, Google's Application, Microsoft Azure etc., give the users in developing applications in cloud setting and to access them from anyplace. Cloud knowledge are keep and accessed in a very remote server with the assistance of services provided by cloud service suppliers. Providing security could be a major concern because the knowledge is transmitted to the remote server over a channel (internet). Before implementing Cloud Computing in a company, security challenges must be self-addressed initial. The researcher has tendency to highlight knowledge connected security challenges in cloud based mostly setting and solutions to beat [7].

M. Khalil and Abdullah Khreishah (2014) targeted on cloud computing is a rising technology paradigm that migrates current technological and computing ideas into utility-like solutions like electricity and water systems. Clouds bring out a good vary of advantages together with configurable computing resources, economic savings, and repair flexibility. However, security and privacy considerations are shown to be the first obstacles to a good adoption of clouds. The new ideas that clouds introduce, like multi-tenancy, resource sharing and outsourcing, produce new challenges to the protection community. Addressing these challenges needs, additionally to the power to cultivate and tune the protection measures developed for ancient computing systems, proposing new security policies, models, and protocols to handle the distinctive cloud security challenges [8].

Rabi Prasad Padhy associated Manas Ranjan Patra(2011) emphasised that cloud computing is an design for providing computing service via the web on demand and pay per use access to a pool of shared resources specifically networks, storage, servers, services and applications, while not physically deed them. Thus it saves managing price and time for organizations. several industries, like banking, attention and education are moving towards the cloud thanks to the potency of services provided by the pay-per-use pattern supported the resources like process power used, transactions applied, information measure consumed, knowledge transferred, or space for storing occupied etc. Cloud computing could be a fully web dependent technology wherever shopper knowledge is keep and maintain within the knowledge center of a cloud supplier like Google, Amazon, Salesforce.som and Microsoft etc.[9].

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. The cloud computing services are provided on demand and payment basis and it is taken back after the usage and terms completion. In this regards security is the main concern about their data storage

and others. The security problem of cloud computing is very important and it can prevent the rapid development of cloud computing. The main objectives of this research paper to identify the security parameters and its significant challenges, issues in cloud computing environment.

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 [10].

1. What are security attributes which 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?

V. CONCEPTUAL FRAMEWORK OF THE RESEARCH STUDY

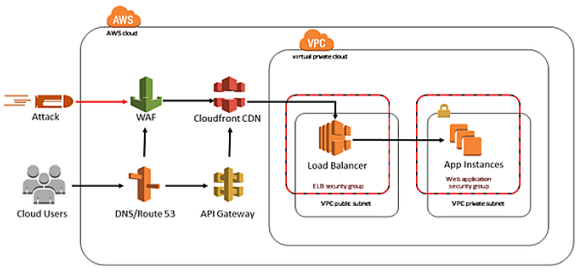

Fig 5.1 : Source - Amazon Case Study: Building a Secure Cloud Computing Environment

VI. DEVELOPING A SECURE COULD COMPUTING ENVIRONMENT

An on-premise datacenter to the general public cloud, hybrid-cloud infrastructure, or are considering either, cyber security ought to be prime of mind. No matter your chosen cloud answer, there are many actions you'll fancy secure the info flowing through your infrastructure. Amazon net Services (AWS) are wont to patterns identification that apply to most public clouds — solely the names of the individual product offerings can amendment. At a minimum, there are 5 practices that ought to be followed in each cloud surroundings handling secure data [11]:

1. Data-encryption at rest and in transit.
2. Multi-factor Authentication.
3. A CDN to assist buffer your net services from DDoS attacks.
4. Adopt CI/CD infrastructure and application security and penetration testing.
5. A web-application firewall or WAF to safeguard your application network traffic.

In today's world of mass-scale fraud and instant electronic transactions, a web user's personal knowledge has become valuable currency among hackers. Variety of federal rules govern the securing of those sorts of knowledge, together with HIPAA for aid knowledge and PCI for electronic transactions. These rules specify that in person recognizable data should be encrypted once at rest in your infrastructure, and whereas in network transport. Securing knowledge at rest includes file storage (AWS's S3), and encrypting information's either via drive volume encoding or through the database API (MySQL). If your storage mechanism doesn't directly support encoding, there are pre-infrastructure choices like AWS's encoding service KMS, or its shopper encoding libraries found here. Securing knowledge throughout transit will typically be

difficult — all services won't support Secure Socket Layer (SSL) or its successor Transport Layer Socket (TLS). These protocols work on the port level to write in code communications between services. Extra choices embrace encoding at the network layer, however which will be valuable and leave you exposed on switches and routers which will not support hardware-based encoding.

VII. CASE STUDY : AMAZON CLOUD COMPUTING SECURITY MODEL

Today's ever-connected world implies that your application surroundings is hospitable attack 24/7/365. No resolution goes to produce a one thousandth guarantee against attacks. It's necessary to know the tools that defend your cloud environments, yet because the strengths and limitations. Produce security best practices that apply to any or all of your environments and deploy and take a look at them in an automatic fashion to extend the possibilities that your applications are ready for the subsequent cyber-attack. It's additionally necessary to understand that cloud security isn't a one-and-done proposition. As your infrastructure and net footprint expands, therefore will your exposure to attack and attractiveness as a target. Once the attacks against your cloud become subtle, it'd be time to speculate in a very qualified security partner and begin victimization additional advanced cloud security tools like Intrusion Protection Services (IPS via agents on your instances) and Intrusion Detection Services (IDS via analytics and observance of your network infrastructure). smart the great the nice} news is that taking precautions too soon along with your application environments is cheap and can begin building good security practices absolute to profit you throughout all stages of growth.

Finally, in today's speedily dynamical world, precaution isn't enough. You wish to be ready to be proactive and take action once attacks target your infrastructure. One among the fashionable tools which will assist you during this could be a net Application Firewall (WAF). A WAF could be a piece of package running on a collection of machines on the far side your application/network load balancers. The package monitors the ports that are listening on your elastic load balancers, and if an outsized volume of information seems or isn't within the right format, the WAF is meant to expand to soak up the attacks so reduce down once they're over or otherwise alleviated. The foremost common sort of cloud design accustomed mitigate these attacks is brought up as a sandwich configuration since it wedges between the cloud and your infrastructure.

Table 7.1: Source: Statista- Security Attributes and Challenges

Cloud Security Attributes	Significant Challenges	Some What of Challenges
Managing Cloud Spend	21%	55%
Security	29%	48%
Compliances	21%	47%
Governance and Control	25%	46%
Lack of Resources /Expertise	27%	46%
Performance	14%	41%
Managing Multiple Clouds	22%	41%
Building a Private Cloud	20%	33%

VIII. STATISTICS OF CHALLENGES OF USING AS CLOUD COMPUTING WORLDWIDE AS OF 2018

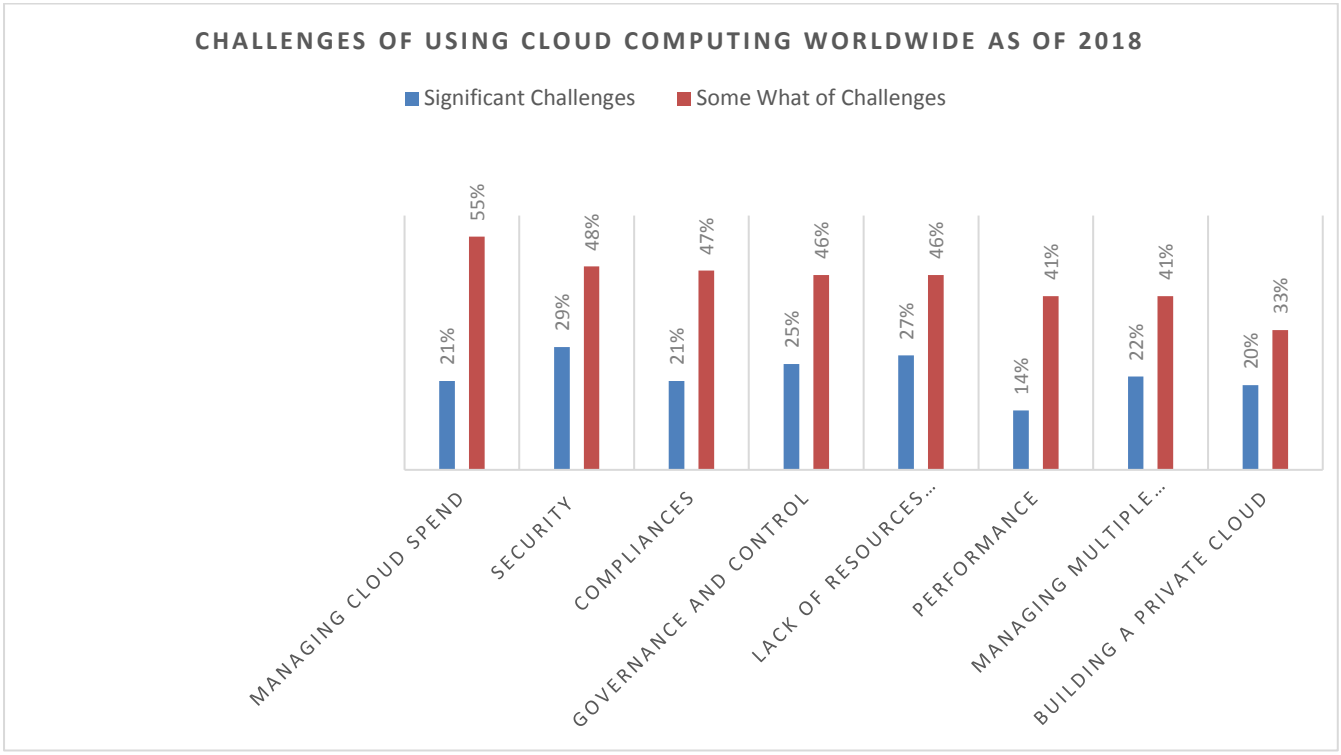

Fig7.1: Source: Statista- Challenges of using cloud computing worldwide as of 2018

STATISTICS: This statistical analysis report shows that the risks of cloud computing for enterprises worldwide, as of 2018, consistent with a Jan 2018 survey conducted by Right Scale. As of Jan 2018, 27% of respondents indicated that a scarcity of resources or experience for cloud computing was a risk of cloud adoption for his or her enterprise or organization with respect to using the cloud computing services.

IX. CONCLUSION

In this research paper the researcher focused on the significant research issues of security as a services in cloud computing environment. The Cloud Computing could be a comparatively new approach that presents a decent variety of advantages for its users who are not having sufficient infrastructure, advancement of software services and platform for their users and organizations. But, due to high demand of computing services it raises some security issues which can hamper its use. The researcher emphasized that vulnerabilities exist in Cloud Computing can facilitate organizations to create the shift towards the Cloud. Since Cloud Computing leverages several technologies, it additionally inherits their security problems. The solution point of view such as ancient net applications, information hosting, and virtualization are looked over, however a number of the solutions offered are immature or inexistent. The researcher got conferred security problems for cloud models: IaaS, PaaS, and IaaS, that vary looking on the model. Storage, virtualization, and networks are the largest security issues in Cloud Computing. Virtualization that permits multiple users to share a physical server is one in all the most important issues for cloud users. Also, another challenge is that there are differing kinds of virtualization technologies, and every sort could approach security mechanisms in numerous ways in which. Virtual networks also are target for a few

attacks particularly once communication with remote virtual machines. The security as a services is still in research and development the enterprises or organizations are not ready to leave their valuable data and information with trust on at third party machine. In this case trust is one of the single attribute to provide assurance of security in cloud computing environment.

X. 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 Takabi And James B.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 Hogben, 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 Urooj Akram (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. Velumadhava Raoa 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 Manas Ranjan 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]. Wentao Liu (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.

Cite this article as :

Dr. Bechoo Lal, Dr. Chandrahauns R Chavan, "Analysis of Cyber Security Solution: Security as a Services (SaaS) in Cloud Computing Environment", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 6 Issue 4, pp. 359-366, July-August 2019.
Journal URL : http://ijsrst.com/IJSRST196492