RESEARCH ARTICLE OPEN ACCESS

Cyber Security on Cloud

Royston, Prem, Sebin, Divik
(Students, St Joseph Evening College, Bangalore)

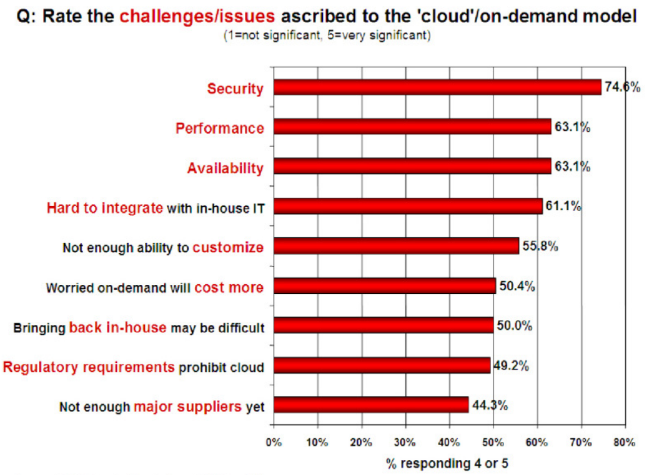
Abstract:
Cloud computing has taken center stage in the present business scenario due to its pay-as-you-use nature, where users need not bother about buying resources like hardware, software, infrastructure, etc. permanently. As much as the technological benefits, cloud computing also has risks involved. At the same time due to its risks, customers -- relatively majority in number, avoid migration towards cloud. This paper analyses the current security challenges in cloud computing environment based on state-of-the-art cloud computing security taxonomies under technological and process-related aspects.

Keywords **—Challenges, Cloud Computing, Security, Techniques**

I. INTRODUCTION

Cloud computing came with the merging of many technologies. Obviously, hardware is required. Relatively low-priced servers and storage makes data centres possible. Increased accessibility and availability of high-speed internet connections means these data centres can be located where it is most economical. Naturally, a data centre alone does not constitute cloud computing. Cloud computing is recognized through the cloud computing stack. The cloud computing stack arranges the hardware/software of a data centre into various service layers. cloud computing is a model for enabling pervasive, convenient, on-demand network access to a shared group of configurable computing resources (e.g., networks, storage, servers, applications, and services) that can be quickly provided and released with less management effort. This cloud model consists of five important characteristics, three service models, and four deployment models. The main idea of cloud computing is to provide both software and hardware as services. There are three layers of services over the cloud.

These are software as a service (saas), platform as a service (paas), and infrastructure as a service (iaas). Individuals and organizations have been considering services over the cloud to cut the costs of expenditure, without any compensation in utilizing recent technologies.



Source: IDC Enterprise Panel, August 2008 n=244

Figure 1: Survey on challenges/issues on cyber security

Survey reports the international data corporation (IDC) conducted a study of 263 it executives and their line-of business colleagues to estimate their views and know their companies use of it cloud services. Security placed first as the greatest challenge of cloud computing. Followed in this paper, section ii discusses security issues in cloud. In section iii, challenges of cloud computing security are being discussed and later sections include conclusion and references.

Research Question 1: what are the various security techniques being used by the leading Cloud Computing providers, to prevent active and passive attacks when the data is being transferred between the Cloud and a local network?

Research Question 2: what are the various security techniques being used to prevent unauthorized access to data within the Cloud?

Research Question 3: what are the major security challenges we expect in future Cloud Computing?

Research Question 4: How can we handle security problems that are expected in future Cloud Computing?

II. SECURITY ISSUES IN CLOUD COMPUTING

Figure 2: Security issues in cloud.

The CSA has warned that the shared nature of cloud computing introduces the possibility of new security breaches that can wipe out any gains made by switching to cloud technology. Cloud computing environment provides users with capabilities to process and store and their data in third- party data centres. Foundations utilize the cloud in a wide range of administration models and arrangement models (private, open, crossover, and group). Security concerns identified with distributed computing condition fall into two classes: Security issues looked by cloud suppliers and Security issues looked by their clients. The liability is shared, however the provider must guarantee that their infrastructure is safe and that their clients' data and applications are secure, while the user must take measures to strengthen their application and use strong passwords and authentication measures. Enterprises are no longer sitting on their hands, doubting if they should risk transferring their sensitive data and applications to the cloud. They're doing it but still the security remains a serious concern. Some security issues are discussed below: Data Breaches: Cloud computing and services are to some extent new but data breaches have been there for years. A study made by the Ponemon Institute entitled “Man in Cloud Attack” reports that over 50 per cent of the IT and security experts surveyed and believed that their association's safety efforts to secure information on cloud administrations are low. The inclusive data breaching was three times more possible to occur Iqra Altaf Mattoo, International Journal of Advanced Research in Computer Science, 8 (2), March 2017 (Special Issue),46-48 © 2015-19, IJARCS All Rights Reserved 47 for businesses that use the cloud rather than those who don’t use the services of cloud. Hijacking of Accounts: Attackers now have the skill to use your login information to distantly access critical data stored on the cloud. Some other methods of hijacking include scripting bugs and reused passwords, which permit attackers to easily steal credentials without detection. In April 2010 Amazon faced a cross-site scripting bug that targeted even the credentials of customers. Insider threat: An attack from inside your organization may seem questionable and doubtful, but the insider threat remains there. Employees can use their authorized access to an organization’s cloud based services to exploit and misuse information such as financial forms, customer accounts, and other critical information. Malware injection: Malware injections are scripts or code that is embedded into cloud services and behave as “valid instances” and run as Software as a service (SaaS) to cloud servers. This means that malicious code could be injected into cloud services and observed as part of the software that is running within the servers of the cloud environment. Once an injection is executed and the cloud begins working with it, attackers can snoop and compromise the integrity of critical information and data. Abuse of cloud services: The cloud’s incomparable storage capacity has permitted both hackers as well as legal users to host and spread malware, illicit software, and other digital assets. These risks consist of sharing of pirated software, music, videos, or books. You can decrease your exposure to risk by continuously monitoring usage and setting strategies for what your employees host in the cloud. Denial of service attacks: Unlike other types of cyber-attacks, which are usually launched to create a long-term foothold and hijack sensitive information, denial of service attacks do not challenge to breach your security perimeter.

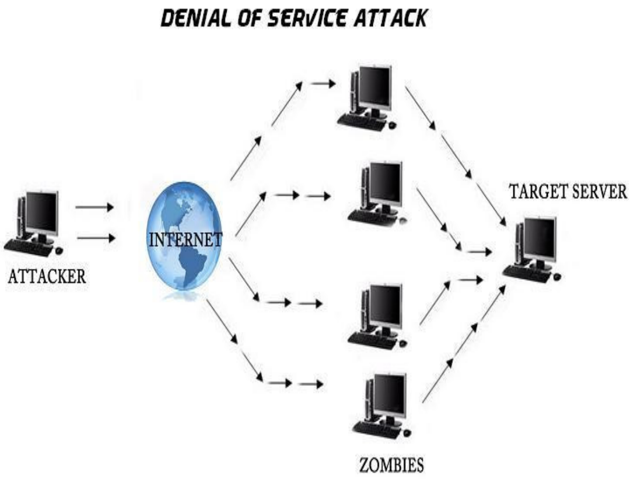


Figure 3: Denial of Service (DOS)

Denial of Service (DOS) Attacks Instead, they try to make your servers and website unavailable to authorized users. In some cases, however, DoS is also used as a mask for other malicious actions, and to take down security applications such as firewalls. Shared vulnerabilities: Cloud security is a mutual relationship between the provider and client. This relationship requires the client to take preventive actions to defend their data. While major providers like Drop box, Box, Microsoft, and Google have consistent measures to secure their side, fine grain control is up to the client. Data Loss: On cloud data can be easily lost through natural disaster, a malicious attack, or a data wipe done by the service provider as shown in figure 2.

The businesses that don't have a recovery plan can get affected very badly if their sensitive data is lost by any means mentioned above. Securing your data means to look over your provider's back up measures or procedures as they relate to physical access, storage locations, and disasters.

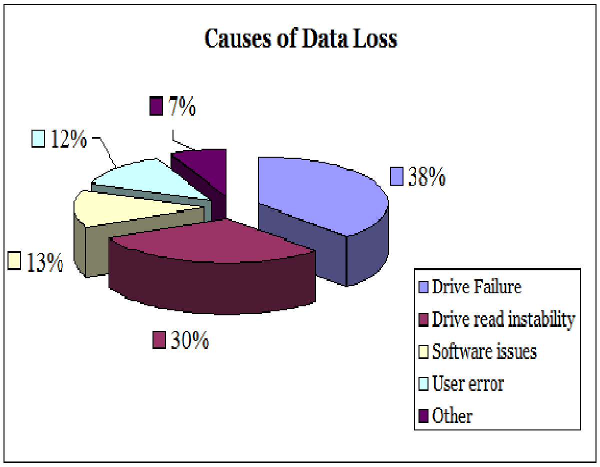


Figure 4: Analysis of Causes of Data Loss.

III. CLOUD COMPUTING CHALLENGE

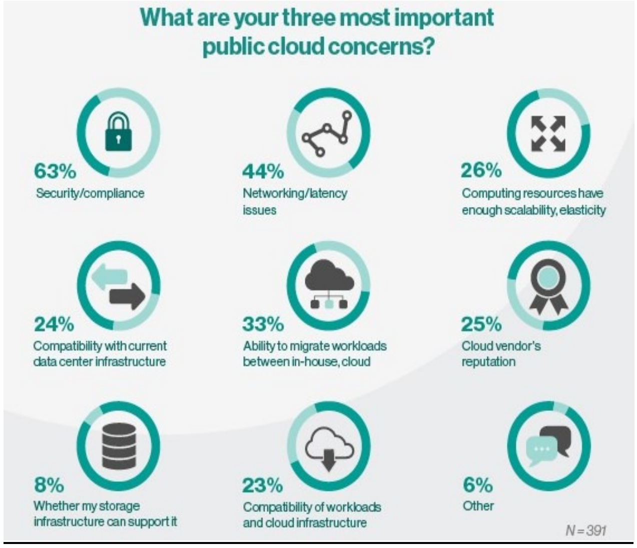


Figure 5: Challenges in Cloud Computing.

The challenges related to cloud computing environment have always been there. Companies are well aware of the business value that cloud computing brings and are taking steps towards switch to the cloud. A smooth changeover involves a thorough understanding of the advantages as well as challenges involved. Like any new technology, the adoption of cloud computing is not free from challenges. Some of the most important challenges are as follows: Security and Privacy: The topmost concern that everybody seems to agree as a challenge with cloud is security. The privacy and data security concerns are on the top of nearly every survey. For instance, hackers can use Cloud to organize botnet as Cloud frequently delivers more reliable infrastructure services at low price for them to start an attack. Interoperability and Portability: Businesses ought to have the energy of moving all through the cloud and changing to various suppliers at whatever point they require. Distributed computing administrations ought to be able to consolidate easily with the on commence IT. What to relocate: Based on an overview (Sample estimate = 244) directed by IDC in 2008, the seven IT frameworks/applications being moved to the cloud are: IT Management Applications (26.2%), synergistic Applications (25.4%), privy Applications (25%), dodge Applications (23.4%), Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). This result reveals that affiliations still have security/assurance stresses in moving their data on to the Cloud. The overview demonstrates that in three-year time, 31.5% of the association will move their Storage Capacity to the cloud. Be that as it may, this number is still generally low contrasted with Collaborative Applications (46.3%) around then. Iqra Altaf Mattoo, International Journal of Advanced Research in Computer Science, 8 (2), March 2017 (Special Issue), 46-48 © 2015-19, IJARCS All Rights Reserved 48 Performance and Bandwidth Cost: Businesses can save some money on hardware but they need to spend more for the bandwidth. This can be a low cost for smaller applications but can be considerably high for the applications that require large amount of data. Delivering complex and demanding data over the network requires sufficient bandwidth. Because of this, many businesses are still waiting for a reduced cost before moving to the cloud

The European Union Agency for Network and Information Security (ENISA) has done significant work in addressing many security issues related to the cloud. It provides stakeholders with information that helps them to understand, assess, and manage the risks when migrating into the clouds. It also provides advisory services on setting and monitoring SLAs to optimize security gains.

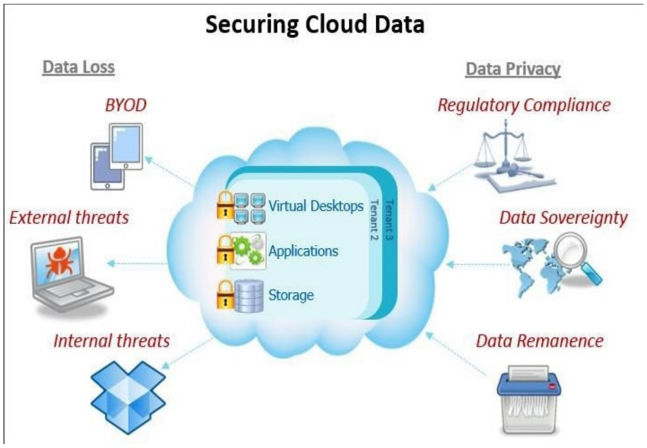


Figure 6: Comparative Evaluation of Well-Known General Cloud Security Mechanisms

ENISA also provides cooperative studies with various stakeholders to identify the critical cloud services and analyse the impact of the cloud service failure in such circumstances. In the following subsections, we present the state-of-the-art general tools that are individually and collectively used to countermeasure cloud security attacks.

IV. INTRUSION DETECTION SYSTEMS (IDS)

Gate crashers, through imitating genuine clients, can get to cloud foundations making it be inaccessible for honest to goodness clients. It has been demonstrated that aggressors can without much of a stretch get data in regards to casualty machines in the IaaS part of the cloud. This data can help in assaulting cloud clients by co-finding the pernicious virtual machine with the casualty's virtual machine. These assaults incorporate dissent of administration (DoS) and dispersed refusal of administration (DDoS) assaults that for the most part target information secrecy, respectability, and accessibility. Such assaults can be kept away from by executing IDS which offers extra safety efforts by exploring system movement, log records and client conduct. IDS is characterized as a framework that gathers and examinations data, from various key focuses, for security inspecting and observing keeping in mind the end goal to check whether this is an infringement of system strategies or not. Interruption recognition can be arranged into two classifications (1) abuse location (MD) and (2) abnormality identification (AD). MD manages data qualities of client's information and making a correlation with database comes about (past contributions by a similar client). Then again, oddity location stores client conduct in include database, which can be contrasted and current conduct. In the event that there is a high rate of distinction in correlation, at that point the attack happened. IDS have two sorts (1) have based IDS (HIDS) which screens the conduct on a solitary host and (2) organize based IDS (NIDS) which investigations activity coursing through a system. Roschke et al. in talk about a third sort called half and half IDS otherwise called disseminated IDS, which joins the elements of both NIDS and HIDS.

The creators in propose an IDS framework named Grid and Cloud Computing Intrusion Detection System (GCCIDS) which depends on NIDS and HIDS. It comprises of a review framework that distinguishes and covers assaults that have not been secured, beforehand, by different NIDS and HIDS frameworks. It works by incorporating information and conduct examination keeping in mind the end goal to distinguish interruptions. The principle parts of GCCIDS incorporate hub, benefit, occasion reviewer and capacity framework. The fundamental impediments in GCCIDS incorporate the high correspondence overhead and excess. Every hub recognizes the nearby occasion and cautions all other associated hubs. The overhead increments drastically when the quantity of hubs increments because of the monstrous calculations and correspondences included. Moreover, GCCIDS does not give any data with reference to whether a hub should instantly caution different hubs as interruption happens or at a specific predefined intermittent time interim. Give us a chance to think about the instance of quick imparting to a framework, for instance, of 1000 hubs. Each time interruption happens, the identifying hub will ready the various 999 hubs producing high overhead of correspondence trade. Aggressors can use this 'ready sharing' as an open window to upset the system. Aggressors carry on as interlopers in various interims of time, setting off specific hubs to recognize these interruptions and subsequently informing different hubs, which extensively expand the correspondence overhead. In the event that a hub chooses not to quickly caution different hubs, irregularity emerges. A hub that distinguishes an assault contains the data about the assault, while different hubs don't know about it. Every hub, in this framework, comprises of a neighbourhood database that has data identified with interruptions happened beforehand. The nearby archive prompts excess.

GCCIDS utilizes information based and behaviour–based methods for assault occurrence recognition. Learning based strategies can't identify new assaults since identification relies upon predefined rules. In any case, this constraint can be eased through consistently refreshing nearby vaults with data about new assaults. For conduct based method, GCCIDS utilizes sustain forward simulated neural system (FFANN). Be that as it may, FFANN isn't helpful at the beginning stage because of next to zero information accessibility. In any case, as the time passes and more calculations are finished by FFANN, the outcomes move forward.

The repetition of archive in GCCIDS has been evacuated in an IDS framework called Distributed, Collaborative and Data driven Intrusion Detection and Prevention system (DCDIDP). DCDIDP makes worldwide database to be utilized for identification errands by the ID counteractive action module. DCDIDP comprises of three level designs, in particular: system, have and worldwide framework. System and host design keep up neighbourhood database of arrangement and guidelines and add to worldwide database. The worldwide database shares data with respect to interruptions among various mists. The fundamental highlights of DCDIDP incorporate being circulated (strategies are dispersed among has), synergistic (has team up with each other to remain synchronized for data sharing) and information driven (dynamic assessment of principles and access list). DCDIDP can be actualized in IaaS, PaaS, and SaaS and gives successful intrusion. Be that as it may, the joint effort among various mists requires a broad confide in administration, which does not exist in the current DCDIDP system. It doesn't give ways to deal with advance trust among cloud clients past what is expressed in SLA. Data sharing among various mists is additionally reliant on the structure of each cloud. At last, DCDIDP has not been assessed and confirmed through handy executions.

Dastjerdi et al. propose another IDS framework by consolidating and stretching out the shared IDS in view of versatile specialists and the conveyed interruption recognition utilizing portable operator (DIDMA). It comprises of four principle parts specifically IDS control focus (IDS CC), office, application particular static operator indicator and specific investigative versatile specialist. IDS CC is focal piece of IDS segment organization. Dastjerdi et al. guarantee that their proposition lessens arrange stack and gives better put stock in administration.

Figure speaks to the general perspective of IDS structure that comprises of NIDS and HIDS. Every id (paying little mind to being conveyed on appropriated systems, framework or cloud) require some essential segments, for example, ready sharing, analyser, method to recognize the suspicious conduct, and so forth. Specialists and experts are giving arrangements, as IDS, DIDS or HIDS, by lessening the quantity of segments and by expanding the execution of IDS. Cloud framework is changing so quickly that present interruption location frameworks are not sufficiently adaptable to adapt to these progressions. One arrangement can be self-ruling IDS that can refresh its strategy when cloud framework changes. A relinquished region here is to create components for conveyed IDS (Network or host based), which include both entomb and intra mists contemplations. Framework heterogeneity, among mists, and utilization of productive correspondence conventions represents another test in cloud security.

A simple approach to follow the gathering paper arranging necessities is to utilize this archive as a format and essentially sort your content into it.

2. In the event that you have to trade delicate or secret data between a program and a web server, Encryption is an undeniable instrument to ensure correspondence. Legitimate encryption of information and encryption of transmission is essential. The relief strategies recognized from the overview is as per the following: SSL (Secure Socket layer) ·

VPN (Virtual Private Network) · IPsec (Internet Protocol Security) · an appropriate utilization of encryption can give great assurance against dynamic assaults. Keeping in mind the end goal to ensure against Man-in-the-centre assaults, one ought to watch if there are any deferred reaction times, so as to recognize if there is any "Go between".

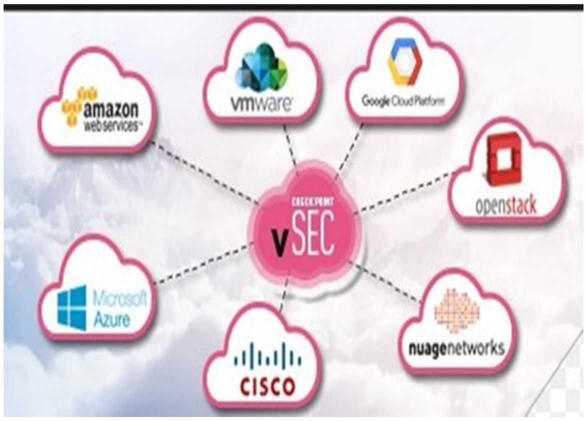


Figure 7: Basic architecture of Intrusion Detection Systems.

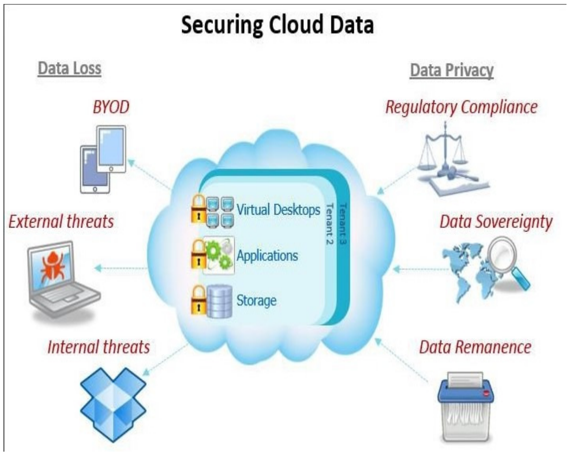


Figure 8: Cloud Security.

A proper use of encryption can give good protection against eavesdropping.· Traffic analysis is harder, but on the other hand, not only that many need protection against this kind of threat. 8.2 For Research Question: 2 we have identified the security techniques that are used in the case of when data resides in the Cloud in Systematic process. The identified challenges, mitigation techniques and compromised attributes are described in Appendix section. The few popular security methods are Secure Socket Layer (SSL) Encryption; Multi Tenancy based Access Control, Intrusion Detection System, Novel Cloud dependability model, Hadoop Distributed File System and Hypervisor. From the analysis of results from survey we have identified the following security challenges 40 Secure identification of users (authentication, e.g. with smart cards or· passwords) Secure communication (e.g. encryption) · Secure IT-infrastructure at the vendor site (e.g. secure domains, firewalls, · virus control, etc...) Secure personnel (e.g. security screening)· Secure audit (e.g. security logs)· Separation of users (e.g. different virtualized zones)· Secure administrative routines for system administration (e.g. separation of· duties) Security education of all IT personnel.· Agreements specifying security rules (between vendor and customer)· Information classification and “Need-to-know”.· If you are pertained about storing sensitive or confidential data in the Cloud, you should encrypt the data before keeping it to the Cloud. 8.3 For Research Question: 3 as the security technology have to improve continuously, in order to meet new security threats. People in common have to be more risk aware and security aware, in order to protect their own information and their company's information. The security challenges have to be faced in future are: Virtual machine security· Trusted transaction· Risk of multiple Cloud tenants· Smart phone data slinging· Hypervisor viruses· Abuse and nefarious use of Cloud Computing· Insecure application programming interfaces· Malicious insiders· Shared technology vulnerabilities· Service and traffic hijacking· Security requirements are complex to specify – When data and services are· moved to the Cloud it becomes even more crucial to be able to specify the security requirements. Information about the security levels of information systems is necessary for efficacious risk management. Security assessment is difficult since the concept of security is vague and cannot be directly measured. Instead other properties and effects of systems have to be measured and combined in order to illustrate the security levels and create the desired information about security. When data and services are moved to the Cloud, security assessment becomes even more challenging since more parties are involved and the systems become more complex.

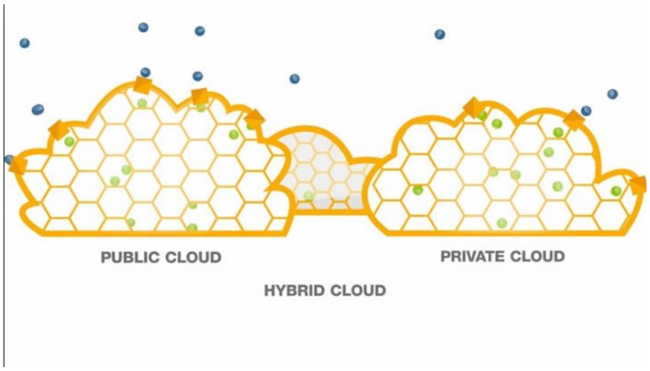


Figure 9: Types of Cloud computing

V. CONCLUSION

The identification of security challenges and mitigation techniques in Cloud Computing is challenged by considering the large number of services. Most of the responses from survey, noted that Cloud Computing will place dominant and expandable information transactions. Because it offers many flexible services, provides easy, individualized and instant access control to the services and information where they are for the users. In the process of identification from the research methods SLR and Survey, we have identified satisfactorily number of challenges and mitigation techniques in current and future Cloud Computing. In spite of the fact that cloud computing can be seen as a new occurrence which is set to metamorphose the way we use the internet, there is much to be careful about. There are many new technologies evolving at a faster rate, each with technological advancements and with the potential of making human lives easier. But, one must be very careful to understand the security risks and challenges posed in utilizing these technologies has many advantages, but it also has different security concerns that could be raised. When data is being stored in big data centres all around the world, the data could eventually become a target for attacks or it could be altered by the employees of cloud service provider. With the advent of this technology, cloud computing was first commercialized and then its pros and cons were taken into consideration.

ACKNOWLEDGEMENT

In this paper, we offer a quantitative model of security estimation that empowers cloud specialist co-ops and cloud supporters of evaluate the dangers they bring with the security of their benefits, and to settle on security related choices on the premise of quantitative examination, instead of mental elements (fear, fears, observations, and so forth.). Our proposed metric offers the accompanying characteristics:

- Security is measured in financial terms, empowering partners to evaluate the dangers they cause because of loss of security, and to settle on choices in like manner.
- Security isn't an inherent characteristic of the framework, yet in addition relies upon partners, and may take distinctive esteems for various partners, contingent upon the stakes they have in the protected operation of the framework

REFERENCES

1. *Madhan Kumar Srinivasan, K. Sarukes, Paul Rodrigues, M. Sai Manoj, P. Revathy, "State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment," Madhan Kumar Srinivasan, K. Sarukes, Paul Rodrigues, M. Sai Manoj, P. Revathy, pp. 470-476 , August 2012.*

2. *Jean-Claude Laprie, Brian Randell, and Carl Landwehr Algirdas Avizienis, "Basic Concepts and Taxonomy of Dependable and Secure Computing," in IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, 2004, pp. 1-23.*

3. *Allan A. Friedman and Darrell M. West, "Privacy and Security in Cloud Computing ," in Issues in Technology Innovation , Brookings , 2010.*

4. *Dr. Daniel Geer. (2003, September) cryptome.org. [Online]. https://cryptome.org/cyberinsecurity.htm*

5. *Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia Michael Armbrust. (2010, April) cacm.acm.org. [Online]. https://cacm.acm.org/magazines/2010/4/81493-a-view-of-cloud-computing/fulltext*

6. *U.Reshma, Dr.V.Praveena S.Sandhya, "Survey on Various Data Encryption Algorithms Used in Cloud Security ," International Journal of Innovative Research in Computer and Communication Engineering , vol. 5, no. 9, September 2017.*