# An Analysis of cyber security and their Impact

**Priya Ghosh, Dr. Arun Kumar Marandi**
*ARKA JAIN University, Jamshedpur-831014, India*
*Email- priyaghoshjsr@gmail.com, arun.m@arkajainuniversity.ac.in,*

***Abstract*** *- This paper discusses the security of data in cloud computing. It is a study of data in the cloud and aspects related to it concerning security. The paper will go in to details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats. Availability of data in the cloud is beneficial for many applications but it poses risks by exposing data to applications which might already have security loopholes in them. Similarly, use of virtualization for cloud computing might risk data when a guest OS is run over a hypervisor without knowing the reliability of the guest OS which might have a security loophole in it. The paper will also provide an insight on data security aspects for Data-in-Transit and Data-at-Rest. The studies, based on all the levels of SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). As the applications of cloud computing are increasing day by day, it is mandatory that both service providers and users make sure that safety, security and privacy covers and mechanisms should be as per the requirements. Cloud computing has become one of the most popular and useful computing model in recent years and benefit of using this computing model is that it is based upon pay as you use system. Security, privacy and protection of data and other resources is one of the significant areas of research in cloud computing.*

*Keyword: - Cloud computing data protection, encryption, digital signature, security issues.*

## I. INTRODUCTION

Cloud Computing (Cloud) provides ubiquitous network access to a poll of resources which are shared and configurable. It is based on shared services and convergence of infrastructure. It emerged from evolution and adoption of many prevalent technologies. It inherits many of its characteristics from client-server model, grid computing, mainframe computing, utility computing, and peer-to-peer architecture. Virtualization is the key technique behind Cloud Computing. It adopts Service Oriented Architecture (SOA) which enables its clients to transform their requirements problems into services thus benefited by the solution provided by the Cloud. Key advantages of cloud include agility, reduced costs, device independence, location independence, easy maintenance, high performance, extremely scalable and flexible, increase productivity, privacy, and security. Cloud computing paradigm is considered as eminently useful and most feasible computing model for the distribution of data, information and resources in a flexible manner. This new computing paradigm accoutres various IT services like storage, computing, security, identity, machine learning and analytics with the help of internet. The nucleus of the research paper is on the assimilation to theoretical concepts with practical implementations of security and privacy strategies that create a secure environment for the service provider and user. This secure environment is beneficial to enhance the level of trust in the end user regarding the cloud services or applications and contrarily for cloud service providers to ensure better and secure services to the users. To achieve sustainable growth and specific goals, cloud service providers have performed the following operations. Cloud computing is the on demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing.

Whether you are running applications that share photos to millions of mobile users or you're supporting the critical operations of your business, a cloud services platform provides rapid access to flexible and low cost IT resources. With cloud computing, you don't need to make large upfront investments in hardware and spend a lot of time on the heavy lifting of managing that hardware. Instead, you can provision exactly the right type and size of computing resources you need to power your newest bright idea or operate your IT department. You can access as many resources as you need, almost instantly, and only pay for what you use.

Cloud computing provides a simple way to access servers, storage, databases and a broad set of application services over the Internet. A Cloud services platform such as Amazon Web Services owns and maintains the network-connected hardware required for these application services, while you provision and use what you need via a web application. Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security.

A. On Demand Self-Service: -It refers to the service which enables provisioning of cloud resources to vendors on demand or whenever they are required such as network storage, service time without the interaction of human.

B. Broad Network Access: - Services are accessible over the network, which are retrieved through some standardized mechanism, which promotes the usage of heterogeneous platforms (workstations tablets, laptops, mobile phones).

C. Resource Pooling: - Resources of cloud Provider are pooled over server. Consumers are assigned different resources, which are either physical or virtual one. Generally, consumer have no idea of exact location the resources provided to them except at the abstraction level like; state, country or data centre.

D. Rapid Elasticity: - Services can be elastically released and monitored, for consumers services available to them can often appear as unlimited which can be scaled in quantity anytime.

E. Measured Services:- Cloud system are so designed that they can monitor the resources usage; for example, processing, bandwidth and active user accounts, storage to deliver transparency to provider as well as consumer. At some level of abstraction, they can optimize the resource usage by keeping a check through metering capability

Cloud Service Models:-

- Infrastructure as a Service (IaaS)
- Software as a Service (SaaS)
- Platform as a Service (PaaS)

Infrastructure as a Service (IaaS): Iaas is all about providing the virtual machine, operating system or networks to the end users. Some other computing resources are also supported in IaaS, where the customer or client can run arbitrary operating system on virtual machines or any other software. Clients can control only the operating system or the software which he is running but he loses his control on the infrastructure which is providing him all these services.

Software as a Service (SaaS): In this kind of scenario, user is only using the applications which are being provided by the vendor and those applications run on the cloud services. Same application is accessible by many other clients as well through some common mechanism, for example by using web browser, or email. Again, the clients or users have no control over the application or underlying infrastructures, network server or operating system upon which these applications run.

Platform as a Service (PaaS): In PaaS, the client is able to create their own desired application by using some programming language, linked libraries. The vendor supports these languages or libraries. After creating the user desired application, it is deployed on the server provided by the vendor. User has also the authority to configure its application or can change the configuration settings later on.

## II. LITERATURE REVIEW

| S.no | Title | Author | Findings | Remarks |
|---|---|---|---|---|
| 1 | Failure Management for Reliable Cloud Computing: A Taxonomy, Model and Future Directions. | Sukhpal Singh and Inderveer Chana etal 2010 | Electronic Health Record(EHR) software runs on the web instead of the computer meaning no hardware or software installation Most cloud based EHR's encrypt the data so hackers cant use the data even if they gain access to it, since the data is stored off site with bank level security Since cloud based servers are maintained off site there are instant reduction in IT cost associated with maintainig the EHR database. The real time data is accessible from multiple location | Failure of cloud computing as tested by the author are software failure which includes complex design,planned/unplanned Reboot, cyber attacks.Hardware failure includes complex circuit design, system breakdown,power outage and other reasons leaving human errors,heat issue etc. |
| 2. | Attribute based Encryption for secure access to cloud based | Maithilee joshi etal 2008 | Its Digital Policy Management where machine specific languages can be used in system in an | Patients data can be compromised if mixed with other clients Not a good option for rural with |

| | | | | |
|---|---|---|---|---|
| | EHR System | | automated one semi-automated manner. Audit Management is for monitoring of behaviour services and adequate analysis and reporting of current and past situation. Identify Management providing service access across multiple external application through single sign on. | limited internet connectivity For long time usage , it may prove to be more expensive A medical practice may lose data if the vendor closes business operation |
| 3. | Security Management areas in the inter cloud | Michael Kretzschmar etal 2011 | Back up data locally Avoid sharing sensitive information Use cloud services that encrypt data | Few practical steps or practises fir a secure cloud experience (could have been included by Author Back up data locally Avoid sharing sensitive information Use cloud services that encrypt data Test he security measures in public Make password storage using special characters |
| 4. | Addressing | Jaypee University | Data Location: When use | The responsibility |
| | Cloud Computing Security Issues and its Solutions | Anoopsahr,Anoopsahr,Uttar Pradesh ,India 2016. | cloud computing services, customers don't know where the data are placed on the servers, even don't know which country these servers are placedin When these countries need to investigate these data, due to the different law, providers may be forced to submit data and be unable to guarantee the security of user data. Data backup: To the important and confidential data, if cloud services dose not backup the data, when data lost by the server problems, or users accidentally delete data, important data can't be restored. | of securing the network is shared between the cloud service provider (CSP) and the enterprise. Depending on which server model an enterprise uses, the enterprise may have little to almost no control over the cloud security. Infrastructure-as-a-Service (IaaS) allows the enterprise to have the most control as the CSP only provides the infrastructure. It falls under the enterprise's jurisdiction to build the remainder of the stack and maintain its security. |
| 5. | Security Issues and their Solution in Cloud Computing | Prince Jain teal. 2017 | Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes | Encryption, authentication and authorization are important components of any security infrastructure, the cloud being no |

| | | | | |
|---|---|---|---|---|
| | | | sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud.There are four types of issues raise while discussing security of a cloud.<br>1. Data Issues<br>2. Privacy issues<br>3. Infected Application<br>4. Security issues | exception. However, since the cloud service provider applies and enforces these security measures, clients feel insecure not knowing which other client also has the same measures in place. One solution is to use different encryption keys for each individual client; however it is wholly dependent on the service provider. |

## III. RELATED WORK

Ayush Agarwal et al. (2016) highlight the emergence of cloud computing along with its security concerns like data loss, data breaches, insecure API's, account hijacking, denial of service [4]. Prachi Garg et al. (2017) have worked on different cloud security aspects like basic security which includes Cross site scripting attacks, Sql injection attacks, Man in the middle attacks [5]. Pradeep Kumar Sharma et al. (2017) security concerns for cloud like cost model charge model [6], service level agreements and issue of migration should be dealt. Naseer Amara et al. (2017) highlighted the security threats, architectural principles and cloud security attacks with their techniques that can minimize the effects of malicious attacks (mitigation techniques) [7]. Sh. Ajoudanian et al, (2012) said that following four parameters were the most crucial. (a) Data Confidentiality, used to avoid leakage of information to any unauthorized individual or system [8].

## IV. METHODOLOGY

The following seven steps outline a simple and effective strategy for finding information for a research paper and documenting the sources you find. Depending on your topic and your familiarity with the library, you may need to rearrange or recycle these steps. Adapt this outline to your needs.

Step 1: Identify and Develop Your Topic- State your topic idea as a question. For example, if you are interested in finding out about use of alcoholic beverages by college students, you might pose the question, "What effect does use of alcoholic beverages have on the health of college students?" Identify the main concepts or keywords in your question. In this case they are alcoholic beverages, health, and college students. Test the main concepts or keywords in your topic by looking them up in the appropriate background sources or by using them as search terms in the Coastal Bend College Library catalog and in online databases such as Literati or CINAHL. If you are finding too much information and too many sources, narrow your topic by using the AND operator: beer AND health AND college students, for example.

Step 2: Find Background Information- Once you have identified the main topic and keywords for your research, find one or more sources of background information to read. These sources will help you understand the broader context of your research and tell you in general terms what is known about your topic. The most common background sources are books and review articles.

Step 3: Use Catalogs to Find Books and Media- Use keyword searching for a narrow or complex search topic. Use subject searching for a broad subject. Print or write down the citation (author, title, etc.) and the location information (call number and library). Note the circulation status. When you pull the book from the shelf, scan the bibliography for additional sources. Watch for book-length bibliographies and annual reviews on your subject; they list citations to hundreds of books and articles in one subject area.

Step 4: Use Databases to Find Journal Articles- Use online databases to find citations to articles. Choose the database that best suits your particular topic; for example, search Literature Online for literary criticism topics, CINAHL for nursing topics, and Academic Search Complete for psychology topics. These databases and more are located on the library's website under Online Resources. If the full text is not linked in the database you are using, write down the citation from the database and search for the title of the journal in the Library Catalog. The catalog lists the print and electronic versions of journals.

Step 5: Find Internet Resources- Use search engines and subject directories to locate materials on the Web. As information on the Internet varies in its reliability, it is suggested that you use directories such as the

Library's Delicious Links [organized by subject] or Google Scholar, which contains links to the library's resources when available.

Step 6: Evaluate What You Find- You may be asked to utilize peer reviewed articles in your assignments. Many journals are peer reviewed, meaning that submitted articles are scrutinized by one or more experts in the field before they are published in the journal. Not all items in a peer reviewed journal have gone through this process, however. These items may include letters, editorials, news, and book reviews. Generally, only the primary articles, such as studies or review articles are peer reviewed.

## V. CONCLUSION AND FUTURE SCOPE

The mechanisms or frameworks, which were suggested for achieving the security, privacy and protection of data and resources in the cloud, revolve around the encryption, forensic and SLA. There is a huge list of questions or queries that remain to be answered. Specific to achieve security and privacy in cloud systems, we identified the challenges and requirements of detecting the hazards and vulnerabilities in the multi-tenant and multi-facet system. We hope that, the efforts made in this research article will be useful for the cloud security/ forensic research community and observations made in this paper will cater to the requirements of the dynamic changing nature of the cloud systems. Increased use of cloud computing for storing data is certainly increasing the trend of improving the ways of storing data in the cloud. Data available in the cloud can be at risk if not protected in a rightful manner. This paper discussed the risks and security threats to data in the cloud and given an overview of three types of security concerns. Virtualization is examined to find out the threats caused by the hypervisor. Similarly, threats caused by Public cloud and multi-tenancy have been discussed. One of the major concerns of this paper was data security and its threats and solutions in cloud computing. Data in different states has been discussed along with the techniques, which are efficient for encrypting the data in the cloud. The study provided an overview of block cipher, stream cipher and hash function, which are used for encrypting the data in the cloud whether, it is at rest or in transit. This paper gave the overview of cloud computing, its various security aspects and keys factors which are affecting the cloud security. Cloud consumer and provider should be sure that their cloud is fully protected. Cloud computing is growing in every industry but it suffers from certain issues regarding security and protection which are a hurdle in its adoption widely. Solutions to these problems have been suggested which can be used for better performance of cloud service.

## VI. REFERENCES

[1]. http://searchvirtualdatacentre.techtarget.co.uk/news/1510117/Community-cloud-Benefitsand-drawbacks.

[2]. Michael glas and paul Andres, “An Oracle white paper in enterprise architecture achieving the cloud computing vision”, CA-U.S.A, Oct 2010.

[3]. Harjit Singh Lamba and Gurdev Singh, “Cloud Computing-Future Framework for emanagement of NGO's”, IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[4]. Dr. Gurdev Singh, Shanu Sood, Amit Sharma, “CM-Measurement Facets for Cloud Performance”, IJCA, , Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[5]. Joachim Schaper, 2010, “Cloud Services”, 4th IEEE International Conference on DEST,Germany.

[6]. Tackle your client’s security issues with cloud computing in 10 steps http :// searchsecuritychannel.techtarget.com/tip /Tackle-your-clients-security-issues-withcloud-computing-in-10-steps.

[7]. Problems Faced by Cloud Computing, Lord CrusAd3r, dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.

[8]. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2),39-51, University of Texas, USA, April-June 2010. H. Erdogmus. Cloud computing: Does Nirvana hide behind the Nebula? IEEE Software.

[9]. B. C. Kaufman and R. Venkatapathy, “Windows Azure TM Security Overview.”

[10]. www.ibm.com/developerworks/websphere/zones/hipods/