Analysis on Cloud Implementations of Security

Naili Dwivedi[1] , Dr. Manmohan Singh[2], Akshay Varkale[3]
[1]M.Tech Scholar, Department of Computer Science and Engineering, IES College of technology Bhopal M.P. India.
[2]Professor, Department of Computer Science and Engineering, IES College of technology Bhopal M.P. India.
[3]Assistant Professor, Department of Computer Science and Engineering, IES College of technology Bhopal M.P. India.
naili.dwivedi98@gmail.com, kumar.manmohan4@gmail.com, varkale.akshay@gmail.com

* Corresponding Author: Naili Dwivedi

Abstract: *Cloud Computing can be classified as a new paradigm for dynamic provisioning computer services supported by data centres that usually employ virtual machine (VM) technology for consolidation. Cloud computing provides infrastructure, platform and software as services that is available to the consumer under the pay as you use model. This paper provides the overview of cloud computing, security issues , challenges in cloud security. Systematic literature review is presented in which several researchers have reviewed the different techniques used for the security of cloud.*

Keywords: *Cloud Computing, Deployment models, Cloud Service Providers*

I. Introduction

Cloud reflects the concept of a distributed system comprising of a group of virtual machines that can be dynamically provisioned to meet the varying resource requirements of a customer and the entire base of this Cloud-Customer relationship is governed by the SLA (Service Level Agreement). The National Institute of Standards and Technology (NIST) [1]defines Cloud as a model that enables convenient on-demand network access to a shared pool of configurable computing resource e.g. network, storage, hardware, applications, etc. that can be rapidly allocated, scaled as well as released with minimum management effort or service provider intervention. Cloud relieves the user of the overhead of physical installation and maintenance of her system, which automatically reduces the overall cost and enhances the system efficiency. Embracement of Cloud based services results in introduction of an abstraction layer between the physical storage or servers and the user whose data or services are being processed in the Cloud.

Data holds the topmost position when it comes to IT security concerns, irrespective of the infrastructure being used. Cloud Computing is no exception to this, moreover it focuses on added security concerns because of its distributed nature and multi-tenant architecture. The data life cycle comprises its generation, storage, usage, distribution and destruction [2]. Each CSP should support all these phases in the data life cycle with appropriate security mechanisms.

Cloud computing has evolved from various technologies that we already know from quite a tie now. These technologies are: virtualization, grid computing, utility computing, web services, internet, www and SOA. Cloud computing is a technology that has changed the way we perform computing. With cloud computing, now everything is in the clouds. By that it is meant that we can develop, deploy and deliver an application in the cloud without having the need of those six digit software licensing, a rapid ROI, and massive decrease in TCO for starting any sized business.

Cloud computing is a model for enabling convenient, on- demand network access to a shared pool of configurable computing resources(such as networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction This cloud model promotes availability and is composed of five essential characteristics, three service models and four deployment models [3].

Cloud computing extends the information technology capabilities by increasing the capacity and adds abilities dynamically without investing on large and expensive infrastructure, licensing software, or training new personals. Among the several benefits, cloud computing provides a more flexible way to access the storage and computation resources on demand. In the last few years, different business companies are increasingly understanding that by tapping the cloud resources and gaining fast access, they are able to reduce their initial business cost by paying only the resources they used rather than the need of potentially large investment (owning and maintenance) on infrastructure. Rapid deployment, cost reduction, and minimal investment are the major factors to employ cloud services that drive many companies.

Cloud computing is authorized through the virtualization technology in which the host system operates an application referred as a hypervisor that generates one or more Virtual Machines (VM) and it faithfully simulates the physical computers. These simulations can be able to operate any software from operating system to the end-user application. The number of physical devices lies in hardware level that includes hard drives, processors and network devices which are placed in the data centers. It is independent of the geographical location that is responsible for processing and storage as needed. The effective management of the servers is performed by the combination of the virtualization layer, software layer, and the management layer. Virtualization layer is utilized to provide the necessary cloud components of rapid elasticity, resource pooling, and location independent. Also, it is an essential element of cloud implementation. The ability to implement security rules and monitoring throughout the cloud is done by the management layer.

II. Cloud Computing Architecture

NIST is responsible for providing security in the cloud computing environment and developing standards and guidelines which shows a valuable contribution that offers a better understanding of cloud services and computing technologies. Cloud computing architecture summarize as the four deployment models: public cloud, private cloud, community cloud, and the hybrid cloud. The deployment models represent the way that the computing infrastructure delivers the cloud services can be employed. The three cloud service models or delivery models are available for the customer: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). There are different levels of security required for these service models in the cloud environment. The wide range of services considered in cloud basic characteristic layer that can be used all over the internet [4]. The cloud service provider is corresponded to provide services, resource allocation management, and security. The architecture explains the five basic components which consist of services that are used in the cloud. The cloud security is the very important and complex task when the data transfer or shared resources to the cloud within the client-server architecture. The architecture of cloud computing is shown in Fig. 1

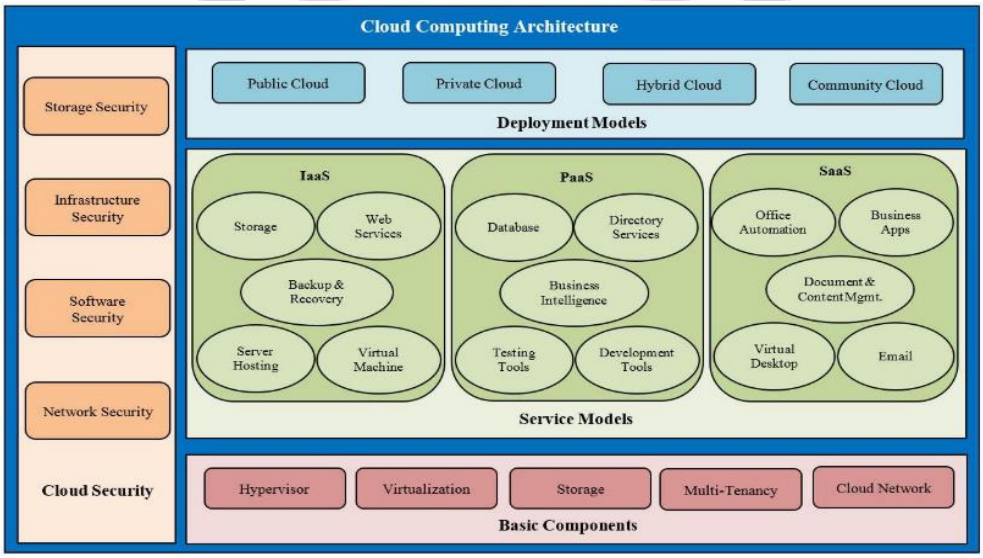

Figure 1 Cloud Computing Architecture [4]

Cloud Computing basically offers three types of services models; Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). SaaS is the highest level of the cloud of which all the services are offered by the cloud providers. Users who adopt PaaS only manage their applications and data and those adopting IaaS will have their infrastructure like server, storage and networking run by the providers. There are three models of deployment – Public Clouds, Private Clouds and Hybrid Cloud. In public clouds, all the services offered by the providers are shared together with all the cloud users. Private clouds are deployed when the users need to enhance their data security to which the clouds are exclusively catered for them. The hybrid cloud is the combination of both public and private clouds. The adoption of these deployment and services offered depends on the needs and requirements of the organization.

Cloud users request for the services from the Cloud Service Providers (CSP). CSPs are third party that providers cloud storage services to their clients. Some other third party service providers are Third-Party Auditor (TPA) and Attribute Authority (AA) that are supposed to provide security functionalities in cloud. As it is known to us that security and trust are the most critical and crucial issues while benefitting the organizations and institutions with cloud. Cloud users data are on high risk which can be lost, leaked or attacked but they do not have any recourse to come out of this substandard situation.

Cloud users do not even aware of to whom they are dealing with or sharing data. Transparency is also a very serious, cloud users do not have any information about the users of their data and how the data is roving inside the cloud. Blockchain is an emerging and novel technology that can be used by cloud users to upsurge the trust and provide security of data while outsourcing and acquiring services from the Cloud. Blockchain can provide advanced security as compared to centralized database security. Blockchain continuously monitors the list of records that are linked and secured using a cryptographic hash function to the previous block.

A blockchain [5] is a distributed ledger that can record transactions and prevents tampering. Blockchain typically managed through peer to peer network and designed to disable arbitrary tampering. Blockchain can provide security at par with the data storage at central database. From management aspects, the data storage damages and attacks can be prevented. Moreover, since the Blockchain has openness attribute, it can provide transparency in data when applied to an area requiring the disclosure of data. Due to such strengths, it can be utilized in diverse areas including the financial sector and the Internet of Things (IoT) environment and its applications are expected to expand. Cloud computing has been applied to many IT environments due to its efficiency and availability. Moreover, cloud security and privacy issues have been discussed in terms of important security aspects.

III. Services Provided by Cloud

The services provided by Cloud also divide it into different types of Cloud. For understanding more about cloud, the services provided by cloud may be given as follows:
Platform as a service (PaaS): This provides environment for applications, development of various preparation tools etc. It provides the runtime environment that controls the applications. This type of Cloud, primarily aims to manage the storage, servers and information systems [6]. It aims to facilitate the management problems related to the application development and also helps the customers.
Infrastructure as a Service (IaaS): This provides the elementary resources access such as virtual machinery, storage, physical machinery etc. The manageable things can be the operating system, application, chosen network elements, application. It actually provides the processing, networks, storage and essential resources for the user.
Software as a service (SaaS): This model provides one o use the application as a service to the users. The network, operating system, servers, storage or applications are not managed by the user. The environment is provided for the software distribution.

IV. Cloud Deployment Models

There are four different types of cloud deployment models [7] which can be named as Public Cloud, Private Cloud, hybrid cloud and community cloud shown in figure 2. The details of these types may be given as follows:
Public Cloud: A cloud infrastructure is managed by a third party and is provided to many customers and which is beyond the firewall of the company. The infrastructure provided, can be used by more than one enterprise at the same time and the resources can be provisioned by users dynamically. The cloud providers are responsible for the management, provisioning, installation and maintenance of the cloud. The cloud providers solely manage and host these clouds.
Private cloud: This type of cloud can be owned or rented and managed by the organization itself or somebody not from the organization that is the third party and exist at on-premises or off-premises. When compared to the public cloud, It is more expensive and secure than it. There are no additional security regulations, legal requirements or bandwidth limitations are there in private cloud that can be present in a public cloud environment also but by using a private cloud, there is control of the infrastructure and improved security at the end of cloud service providers and the clients have optimized, since the user's access and the networks used are restricted.

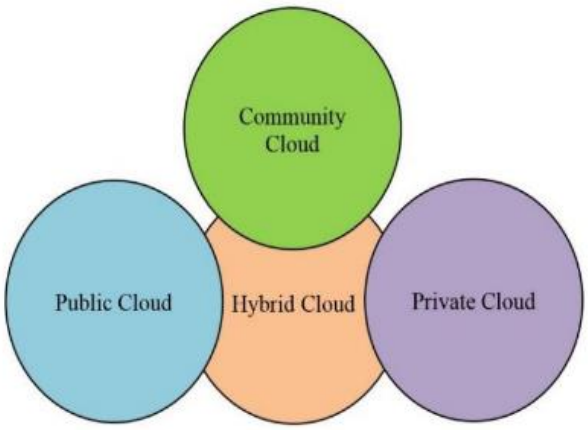

Figure 2 Cloud Deployment Models

Hybrid Cloud: It is a combination of two or more cloud deployment models, linked in such a way that data transferred, takes place between the two different clouds without affecting each other. These clouds would typically be generated by the enterprise and responsibilities for management would be split amongst the enterprise and the cloud provider.
Community Cloud: Infrastructure shared by several organizations for a shared cause and may be managed by a third party service provider or them and rarely offered cloud model. These clouds are based normally on an agreement between business organizations which are related such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook.
LITERATURE REVIEWS
An overview and study of cloud computing, with several security threats, security issues, currently used cloud technologies and countermeasures are presented in [8]. The security challenges in cloud computing are formidable, especially for public clouds whose infrastructure and computational resources are owned by an outside party that sells those services to the general public. Cloud security requirements have been addressed in publications earlier, but it is still difficult to estimate what kinds of requirements have been researched most, and which are still under-researched.
Deep learning is an advanced technique developed to act like that of the human neurological analysis on several problems. Implementation of deep learning algorithm to the cloud security module identifies the movement of malware and spywares in the cloud storage. Similarly the cryptography is an old technique structured to hide the information with a cover data or cover image. It allows the hacking algorithm to extract only the useless data. Article [9] reviews the recent advancements in the cloud security with blockchain, deep learning and cryptographic models.

Cloud Computing is a model based on computing system which provides convenient and customizable services to the users for accessing to different cloud applications. Authors in [10] took all of the elements like security issues, countermeasures for security and concept of cloud security into consideration so that the necessary areas were properly connected and a number of open issues were discussed in this area. They also reviewed the most significant security techniques to data protection and cloud security in the cloud computing. Moreover, security techniques for data protection will be recommended in order to have enhanced security in cloud computing. It will concentrate primarily on issues related to data security and provides solutions.

One of the key difficulties that instructive establishments confront in embracing Cloud computing advances is a provisioning of a protected cloud foundation. In [11], the creators find some cloud benefits in the instruction segment and talk about restrictions of fundamental cloud benefits and in addition highlight security challenges that organizations confront when using cloud innovations. The review was led in assortment instructive establishments to concentrate the perspectives of partners on the cloud security vulnerabilities and methodologies used to overcome.

Healthcare sector is information critical industry that deals with human lives. Transforming from traditional paper based to Electronic Health Records (EHRs) was not efficient enough since EHRs require resources, integration, maintenance and high cost implementation. Cloud computing paradigm offers flexible, cost effective, collaborative, multi-tenant infrastructure which assists in transforming electronic healthcare to smart healthcare that consists on the use of latest technologies such as smart mobiles, smart cards, robots, sensors and Tele-health systems via internet on pay-per-use basis for best medical practices. Cloud computing reduces the cost of EHRs in terms of ownership and IT maintenance, also it offers sharing, integration and management of EHRs as well as tracking patients and diseases more efficiently and effectively. [12] represents the significance and opportunities for implementing cloud computing in healthcare sector. Below in table 1, the paper presents the recent contribution of researchers for deployment of cloud security.

Table 1. Recent Research Contributions

References	Work done	Technique Used	Results
[5]	Reviewed various aspects of security in Blockchain and Cloud Computing and	Cryptographic algorithms	This paper reviewed the various existing blockchain implementations for Cloud security.
[13]	Big data is one of the most problems that researchers try to solve it with perfect security.	Vormetric Concept	Using the Vormetric Toolkit is easily to deploy, integrate and manage the Vormetric Data Security implementation with the rest of your big data implementation.
[9]	Reviewed the recent advancements in the cloud security with blockchain, deep learning and cryptographic models.	Deep learning algorithm with blockchain or cryptographic	A combination of deep learning algorithm with blockchain or cryptography algorithm will improve the combined security issues of the cloud infrastructure.
[14]	Reviewed new developments in the areas of orchestration, resource control, physical hardware, and cloud service management layers of a cloud provider	Review of existing research was conducted to summarize the state-of-the-art in the field	Security and privacy factors that affect the activities of cloud providers in relation to the legal processioning.
[15]	Reviews cloud computing paradigm in terms of its historical evolution, concepts, technology, tools and various challenges	➢ Description of cloud platforms by different CSPs. ➢ Open source tools and commercial tools.	Security objectives and security issues related to the location of data centres, network and other common issues are discussed
[16]	Highlight the possible	Analysis of the Service	A secure cloud computing

	security issues and vulnerabilities connected with virtualization infrastructure	Level Agreement that builds trust between cloud providers and cloud customers	environment depends on identifying security solutions
[17]	Security issues necessities and challenges that cloud service providers (CSP)and user face in cloud atmosphere are discussed	Cloud security and privacy issues which are putting cloud a little back step	Provided the survey report done be several organization in several cloud security prone areas, with their appropriate flowchart and diagram.
[18]	Systematic Literature Review (SLR) of ML and Cloud security methodologies and techniques	Reviewed Cloud security area, type of ML techniques used, and the accuracy estimation of the ML model	The most popular ML used is SVM in both hybrid and standalone models
[19]	Focus on getting well knowledge about Ontology implementation of cloud computing for distributed systems, and explaining the main requirements of performing best ontology.	Ontology Implementation in cloud computing	The quintessence of using ontology in cloud computing consists of reduced time, quick discovery action, and arriving at accurate results

V. Conclusion

The distribution of computing resources is done using a new technology called Cloud Computing. The efficient computing and storage can be achieved in an adaptable manner with the services offered by Cloud. The industry has welcomed this technology for achieving the change in information technology but there are risks associated with this technology. The work has processed to avoid such risks and to overcome them. Cloud computing as of now we know that it refers to the sustained storage and the advanced sharing of data over the internet. But, the threats from the security is embedded in cloud computing approach is proportional to the offered advantages directly. Also, it allows the users to store the data privately as per the requirement.

REFERENCES

[1] Ullah, R., Roy, A., & Basu, S. (n.d.). Cloud Computing Security Challenges & Solutions-A Survey Cloud Computing Security Challenges & Solutions-A Survey.

[2] Security, C. (2014). Cloud Security: Theory and Practice. 1–3.

[3] Faheem, M., Akram, U., Khan, I., Naqeeb, S., Shahzad, A., & Ullah, A. (2017). Cloud Computing Environment and Security Challenges: A Review. International Journal of Advanced Computer Science and Applications, 8(10). https://doi.org/10.14569/ijacsa.2017.081025

[4] Amron, M. T., Ibrahim, R., & Chuprat, S. (2017). A Review on Cloud Computing Acceptance Factors. Procedia Computer Science, 124, 639–646. https://doi.org/10.1016/j.procs.2017.12.200

[5] Srilakshmi, K., & Bhargavi, P. (2019). Cloud Computing Security Using Cryptographic Algorithms. Asian Journal of Computer Science and Technology, 8(S3), 76–80. https://doi.org/10.51983/ajcst-2019.8.s3.2082

[6] Rebollo, O., Mellado, D., & Fernández-Medina, E. (2011). A comparative review of cloud security proposals with ISO/IEC 27002. Proceedings of the 8th International Workshop on Security in Information Systems, WOSIS 2011, in Conjunction with ICEIS 2011, 3–12. https://doi.org/10.5220/0003546900030012

[7] Narang, A. (2017). A Review- Cloud and Cloud Security. International Journal of Computer Science and Mobile Computing, 6(1), 178–181.

[8] Taneja, D., & Tyagi, S. S. (2017). Information Security in Cloud Computing: A systematic Literature Review and Analysis. International Journal of Scientific Engineering and Technology, 6(1), 2277–1581.

[9] Andi, H. K. (2022). Estimating the Role of Blockchain, Deep Learning and Cryptography algorithms in Cloud Security. Journal of Trends in Computer Science and Smart Technology, 3(4), 305–313. https://doi.org/10.36548/jtcsst.2021.4.006

[10] Alsaadi, E. M. T. A., Fayadh, S. M., & Alabaichi, A. (2020). A review on security challenges and approaches in the cloud computing. AIP Conference Proceedings, 2290(December). https://doi.org/10.1063/5.0027460

[11] Rajesh, M. (2017). a Systematic Review of Cloud Security Challenges in Higher Education. The Online Journal of Distance Education and E-Learning, 5(4), 1–10.

[12] Institute of Electrical and Electronics Engineers., & Birla Institute of Technology and Science. (2012). Proceedings of 2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM-12) : December 8-10, 2012, Birla Institute of Technology & Science, Pilani Dubai Campus.

[13] A Y E D Ali, E. S., Assuncao, M., Ooko, J., Sayed Ali Ahmed, E., & ASaeed, R. (2014). A Survey of Big Data Cloud Computing Security Related papers BDC Trends JPDC Big Dat a comput ing and clouds: Trends and fut ure direct ions A Survey of Big Data Cloud Computing Security. International Journal of Computer Science and Software Engineering (IJCSSE), 3(1). www.IJCSSE.org

[14] Gholami, A., & Laure, E. (2015). Security and Privacy of Sensitive Data in Cloud Computing : A Survey of Recent Developments. 131–150. https://doi.org/10.5121/csit.2015.51611

[15] Birje, M., Challagidad, P., Tapale, M. T., & Goudar, R. H. (2015). Security Issues and Countermeasures in Cloud Computing Cloud computing review : concepts , technology , challenges and security. June 2020.

[16] Chandrahasan, R. K., Priya, S., & Arockiam, L. (2012). Research Challenges and Security Issues in Cloud Computing. International Journal of Computational Intelligence and Information Security, 3(3), 42. https://www.researchgate.net/publication/265401218

[17] Nishad, L. S., Pandey, R., Akriti, Beniwal, S., Paliwal, J., & Kumar, S. (2016). Security, privacy issues and challenges in cloud computing: A survey. ACM International Conference Proceeding Series, 04-05-March-2016. https://doi.org/10.1145/2905055.2905253

[18] Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine Learning for Cloud Security: A Systematic Review. IEEE Access, 9, 20717–20735. https://doi.org/10.1109/ACCESS.2021.3054129

[19] Sharma, P. K., Kaushik, P. S., Agarwal, P., Jain, P., Agarwal, S., & Dixit, K. (2017). Issues and challenges of data security in a cloud computing environment. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017, 2018-January, 560–566. https://doi.org/10.1109/UEMCON.2017.8249113

[20] Ageed, Z. S., Ibrahim, R. K., & Sadeeq, M. A. M. (2020). Unified Ontology Implementation of Cloud Computing for Distributed Systems. Current Journal of Applied Science and Technology, November, 82–97. https://doi.org/10.9734/cjast/2020/v39i3431039

[21] Patel, A., Shah, N., Ramoliya, D., & Nayak, A. (2020). A detailed review of Cloud Security: Issues, Threats Attacks. Proceedings of the 4th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2020, 758–764. https://doi.org/10.1109/ICECA49313.2020.9297572

[22] Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A Comprehensive Survey on Security in Cloud Computing. Procedia Computer Science, 110(2012), 465–472. https://doi.org/10.1016/j.procs.2017.06.124

[23] Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, 33, 1–48. https://doi.org/10.1016/j.cosrev.2019.05.002

[24] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88–115. https://doi.org/10.1016/j.jnca.2016.11.027

[25] Paxton, N. C. (2017). Cloud security: A review of current issues and proposed solutions. Proceedings - 2016 IEEE 2nd International Conference on Collaboration and Internet Computing, IEEE CIC 2016, 452–455. https://doi.org/10.1109/CIC.2016.066