International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 10, pp: 388-392 www.ijaem.net ISSN: 2395-5252

Security in Cloud Computing

Divya Rajendra Mali.
Research Student, Department of Information Technology,
B. K. Birla College of Arts, Science and Commerce (Autonomous), Kalyan.

Date of Submission: 20-11-2020 Date of Acceptance: 10-12-2020

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 bstract— 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 bstract— 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 bstract— 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 This paper discusses the security of datain cloud computing. It is a study of data in cloud and aspects related to it concerning security. This 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. Cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply, whilst reducing capital expenditure. However, the opportunity cost of the successful implementation of Cloud computing is to effectively manage the security in the cloud applications. Security consciousness and concerns arise as soon as one begins to run applications beyond the designated firewall and move closer towards the public domain. The purpose of the paper is to provide an overall security perspective of Cloud computing with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of Cloud computing. Gartner's list on cloud security issues, as well the findings from the International Data Corporation enterprise panel survey based on cloud threats, will be discussed in this paper.

Keywords: Cloud computing, Security, Public cloud, Private cloud, Hybrid Cloud, Data protection, Risks and threats

I. INTRODUCTION

Cloud computing is latest trend in IT world. It is Internet-based computing, whereby shared resources, software and information, are provided to computers and other devices on-demand, like the electric grid. This technology has the capacity to admittance a common collection of resources on request. It is proving extremely striking to cash-strapped IT departments that are wanted to deliver better services under pressure. In recent years cloud computing has become a growing interest for organizations looking to reduce their IT costs by offloading infrastructure and software costs onto 3rd party organizations who offer software-as-a-service (SaaS) (e.g.Google Apps), platform-as-a-service (PaaS) (e.g. Google App Engine), and infrastructure-as-a-service (IaaS) (e.g. Amazon EC2).

A major concern in adaptation of cloud for data is security and privacy. It is very important for the cloud service to ensure the data integrity, privacy and protection. For this purpose, several service providers are using different policies and mechanism that depend upon the nature, type and size of data.

One of the advantages of Cloud Computing is that data can be shared among various organizations. In order to avoid potential risk to data, it is necessary to protect data repositories.One of the key questions while using cloud for storing data is whether to use a third-party cloud service or create an internal organizational cloud.

This paper is the study of data security techniques used for protecting and securing data in

cloud throughout the world. It discusses the potential threats to data in the cloud and their solutions adopted by various service providers to safeguard data.

II. OBJECTIVES

To understand the security issues and to identify the appropriate security techniques those are being used in the current world of Cloud Computing.
To identify the security challenges those are expected in the future of Cloud Computing

III. LITERATURE REVIEW

In order to understand the basics of cloud computing and storing data securing on the cloud, several resources have been consulted. This section provides a review of literature to set a foundation of discussing various data security aspects. 1.The study starts by identifying cloud computing security issues, challenges and their mitigation strategies from the literature.2.The design of cloud computing architecture should be attractive.AES is one the most efficient symmetric algorithm. The Advantages It provides strong security from attackers.3.The performance evaluation shows that AES cryptography can be used for data security. Moreover, delay calculation of data encryption shows that larger size of data increases the data delay time for encrypting data.4.A network solution for providing inexpensive, reliable, easy and simple access to IT resources.A major concern in adaptation of cloud for data is security and privacy. It is very important for the cloud service to ensure the data integrity, privacy and protection.Data security in cloud computing involves more than data encryption.5.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.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.6.Cloud computing is the dynamic delivery of information technology resources and capabilities as a service over the Internet.Data Breaches is another important security issue to be concentrated in cloud.7.Cloud computing has become a fundamental part of the computing world.The study concludes that storage, virtualization, and networks are the major security concerns in Cloud Computing.8.At present, there are relevant legal professions in foreign countries, such as the HIPAA (Health Insurance Portability and Accountability Act) and FAPA (Financial Agency Privacy Act), which required relevant units to protect the privacy of clients.9.In the cloud, the owners are not able to control the data that can be executed on the platform. CP-ABE algorithm is quite popular in the cloud environment.When a user stores its data in cloud, it's always a matter of concern if the CSP is providing proper security and privacy to the user, and if the data is not mishandled and misused.10.In 1995, Bill Gates wrote a memo entitled "The internet tidalwave" which described how the internet was going to forever change the landscape of computing.Public clouds are the most commonly used; their resources are made available to the general public by a particular provider, such as Microsoft, IBM or Google.11.CCT is based on several IT innovations, including virtualization, the increasing capacity of the Internet, and the growing sophistication of Internet-based technologies.Cloud computing emerges as a quickly evolving technology that ever more companies are willing to adopt in order to improve collaboration.12.In order to solve the data security problem of the medical cloud platform, it is necessary to combine the access control policy with the encryption mechanism to deal with the privacy leakage problem of data storage procedures in the cloud environment.13.Mobile cloud computing (MCC) has been widely recognized as a promising approach for next-generation pervasive healthcare solutions.The collaborative working of sensors and mobile devices also plays an important role in mobile cloud-based healthcare.Choh et al. proposed a HTTP 2.0 based network infrastructure for mobile cloud health, which enabled secure and fast transmission of medical information to individual users. De et al. and Mukherjee incorporated the femtocell into mobile cloud systems.14. Tjoa, A.M and Huemer the privacy issue by preserving data control to the end user to surge confidence. Several Cloud computing attacks are reviewed and some solutions are proposed to overcome these attacks. 15.This study presents the popular optimization approaches on MCC for meeting the diverse priorities and achieving the optimal tradeoff among multiple objectives.Our work paves the way for future research on employing mobile cloud computing to provide smart, tailored and effective healthcare services.16. Therefore, Abdelkader and Etriby propose a data security model for cloud computing based on cloud architecture. They also developed software to enrich the effort in Data Security model for cloud computing.

IV. METHODOLOGY

This study is based on the secondary data derived from various research papers related to the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 10, pp: 388-392 www.ijaem.net ISSN: 2395-5252

security in cloud computing. This paper discusses the security of data in cloud computing. It is study of data in cloud and aspects related to it concerning security. This 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. A study was conducted to know people's interests and experience with the cloud computing security and also the problems faced during data storage. This study was conducted through google forms which circulated randomly through the study doesn't need any specific population but apopulation that faces some issues in using an any application for the security and data storage. Google forms were the source for conducting the survey. The survey population includes citizens, students. A google form was chosen as a medium to conduct the survey. The google form was circulated for 1 week which resulted in a set of 43 responses.

V. EXPERIMENT

Cloud computing is a new paradigm. In total, we got 43 number of partially and completed responses from the real time survey. However, many do have relevant experience in cloud computing and IT security. Data collected from the people in the form of the survey. Total 43 people were taken part in the survey. According to the survey many people don't know about the cloud computing. Also, many people were not heard about the cloud computing, they don't know that they are using a cloud computing security application in day-to-day life. According to first analysis i.e fig1 we can see that 34.9 people don't know about cloud computing and their security.

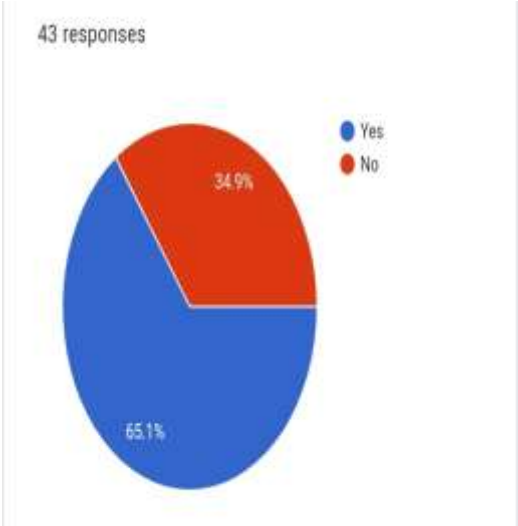

Fig.1

According to second analysis of survey data we can see in fig.2 that I am asking for AWS i.e Amazon Web Service many people (69.8) know about this (as shown in the fig2) and also in the survey some people (46.5) don't know that they using cloud security in day-to-day life using many applications like What's app, Facebook, Netflix (as shown in fig3). Almost all peoples in the survey (97.7) using the applications like What's app, Netflix regularly but they don't know that those applications are secure their data with the help ofcloud computing security. In cloud computing security data is safe and secure strictly. And many people know many cloud security services and secure storage like sync.com, pcloud.com and so many.

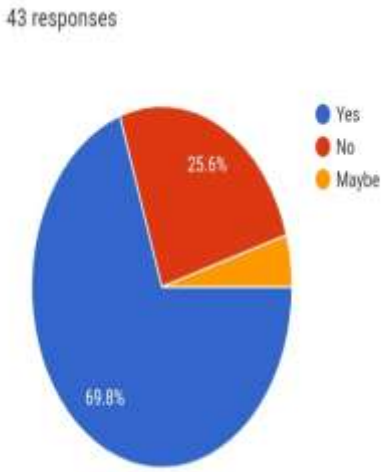

Fig.2

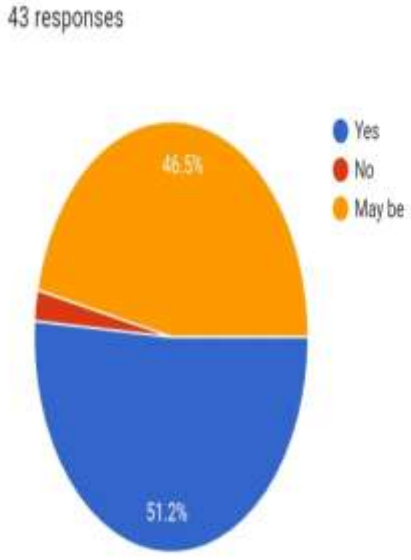

Fig.3

VI. RESULT

From above analysis it is proved that cloud computing is best medium for securing data and secure a data storage. By using cloud computing security, your data will be strictly secure and safe. Many hardware and software are provided for security reasons, but they are not safe and confident about security. Cloud computing security is one of the best option to secure a application, data and our personal data with help of many cloud security services. So, finally all above information we concluded that yes, it is a best security option for data encryption.

So, we predicted that this cloud security is very much useful for many companies and normal user also for secure their data and storage as compare to other hardware and software security services.

VII. CONCLUSION

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 multitenancy 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 use 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 multitenancy 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 use There are many benefits of using cloud computing such as cost efficiency, quick deployment, improved accessibility etc.Increased useof cloud computing for storingdata 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 multitenancy have been discussed. One of the major concerns of this paper was datasecurity and itsthreats 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.

ACKNOWLEDGEMENT

I would like to give special thanks to prof. Swapna Nikale, Department of Information Technology B. K. Birla college (Autonomous) Kalyan, for valuable suggestion in research work and thankful to the participants who responded to the survey.

REFERENCES

[1]. B. Lee, E. K. Dewi and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," 2018 27th Wireless and Optical Communication Conference (WOCC), Hualien, 2018, pp. 1-5, doi: 10.1109/WOCC.2018.8372705.https://doi.org/10.5374/idmsd.2019.11456

[2]. R, Y. R., & K.P, K. (2019). Secure Cloud Data Computing Using Different Algorithms. Journal of Advanced Research in Dynamical and Control Systems, 11(12), 111–116. https:// doi.org/10.5373 /jardcs/v11i12/ 20193219vv

[3]. Kakkad, V., Patel, M., & Shah, M. (2019). Biometric authentication and image encryption for image security in cloud framework. Multiscale and Multidisciplinary Modeling, Experiments and Design, 2(4), 233–248. https://doi.org/10.1007/s41939-019-00049-y

[4]. Zhang, F., Chen, Y., Meng, W., & Wu, Q. (2019). HYBRID ENCRYPTION ALGORITHMS FOR MEDICAL DATA STORAGE SECURITY IN CLOUD DATABASE. International Journal of

Database Management Systems, 11(01), 57–73. https://doi.org/10.5121/ijdms.2019.11104

[5]. Tanweer Alam. Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2 April), 108-115, 2020. DOI: https://doi.org/10.34306/itsdi.v1i2.103

[6]. Annane, B., & Ghazali, O. (2019). Virtualization-Based Security Techniques on Mobile Cloud Computing: Research Gaps and Challenges. International Journal of Interactive Mobile Technologies (IJIM), 13(04), 20. https://doi.org/10.3991/ijim.v13i04.10515

[7]. Chakraborty, M. (2019). Fog Computing Vs. Cloud Computing. SSRN Electronic Journal, 3–8. https://doi.org/10.2139/ssrn.3414500

[8]. 8.Attaran, M., & Woods, J. (2018). Cloud computing technology: improving small business performance using the Internet. Journal of Small Business & Entrepreneurship, 31(6), 495–519. https://doi.org/10.1080/08276331.2018.1466850

[9]. Shen, J., Deng, X., & Xu, Z. (2019). Multi-security-level cloud storage system based on improved proxy re-encryption. EURASIP Journal on Wireless Communications and Networking, 2019(1), 100–500. https://doi.org/10.1186/s13638-019-1614-y

[10]. A. Albugmi, M. O. Alassafi, R. Walters and G. Wills, "Data security in cloud computing," 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), Luton, 2016, pp. 55-59, doi: 10.1109/FGCT.2016.7605062.https://doi.org/10.1080/08276331.2018.1466850

.