International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206123

Cloud Computing Security using by Applying Cryptography Technique

Rajesh Keshavrao Sadavarte[1], Dr. G. D. Kurundkar[2]
[1]Assistant Professor and Head, Netaji Subhashchandra Bose College, Nanded, Maharashtra, India
[2]Assistant Professor, Computer Science Department, Shri. Guru Buddhiswami Mahavidyalaya, Purna District Parbhani, Maharashtra, India
Author Correspondence :sadavarte2003@yahoo.com, gajanan.kurankar@gmail.com

ABSTRACT

Cloud computing is the provision of computing and storage capacity to users as a service. Cloud storage is a type of networked online storage where data is stored in virtualized storage pools as a subservice of infrastructure as a service (IaaS) in cloud computing. Cloud computing plays a significant role in the efficient use of resources and in the utilization of service. Regardless of the cloud category (e.g. private, public, hybrid or inter-cloud), all service providers rely on domain server data. As a rapid development and deployment of cloud computing and cloud storage, users are increasingly concerned about security and privacy issues involved in these techniques. This paper provides a summary of basic security problems that consist of conventional security issues. It also addresses the additional challenges resulting from the cloud computing paradigm being used by cloud system providers and consumers. In addition, solutions suggested by some researchers are presented with a focus on cryptographic techniques which support secure storage of the cloud.

Keywords : Cloud Computing, Cryptography Techniques, Encryption, Cloud Security, Cloud Storage, Security, Privacy

I. INTRODUCTION

While considered a productive or non-profitable enterprise, the concentrated use of capital increases the economic impact and creates tremendous losses. To address this shortcoming, each consumer is hunting for a new technology to solve their demand with minimal effort. The cloud computing provides an excellent platform over the network for resource seekers in this way. The cloud service providers are not considered by most groups to be the secure way of data processing within the public cloud. Yet, at the same time, private cloud is paying more attention to ensuring that the data remains in its cloud servers as well as keeping sensitive cloud data secure. The general framework for cloud storage consists of two main components, such as data and its applications. Both data and applications are handled with the help of cloud data proprietors and cloud service providers (L, Prateelk, & Singh, 2014).

Cloud computing is an evolving technology but it has drawn significant attention from cloud users and cloud providers to its security and privacy risks. One of the main reasons for this is that cloud users must trust the security mechanisms and configuration of the cloud provider and cloud client themselves. Cryptographic technique is currently being treated in the industry and academia community as one of the primary techniques for solving security and privacy problems in the cloud computing environment. In recent years, many types of cryptography-based cloud computing

solutions have been proposed in Ref., focusing primarily on secure storage , secure computing, and secure service usage (Sheik & Komati, 2018).

II. METHODS AND MATERIAL

1. Cloud computing security

A. Trust

Trust is described as the "act of trusting and relying on someone or something to behave as promised". In computing science, faith goes through many fields, such as computer network protection and access control, distributed device reliability, etc. The fact that data and software are outsourced in a cloud environment assigns their power to the cloud provider out of the strict owner control. Consequently, Trust is based on both the delivery model and the cloud provider(D & D, 2012)

B. Cloud security issues

Most conventional security issues are effectively countered because of the innovative architecture of cloud computing. However, the unique characteristics of its infrastructure have brought in a range of distinctive security challenges. In general, security is related to the AIC triad, namely, Availability, Integrity, and Privacy. In particular in the case of cloud computing architecture, these three properties have become key aspects used in the design of secure systems.

1) Confidentiality: This only applies to approved parties or systems with the ability to access protected data. Outsourcing data, delegating power to a cloud provider and making it accessible to various parties increases the risk of data breaches. A variety of questions arise concerning multi-tenancy problems, data remanence , security of application and privacy. Multi-tenancy refers to the resource sharing feature in the cloud. The cloud computing architecture consists of sharing different kinds of resources to allow multiple clients to concurrently use the same resource which poses a number of threats to privacy and confidentiality(Cloud Security Alliance, 2010).

2) Integrity: It means that only approved parties may change assets in the manner permitted and refers to data, software and hardware. Data Integrity refers to protecting data against unauthorized deletion, modification or manufacture. Authorization is the system's mechanism to decide what level of access a single authenticated user should have to protected resources. Because of the growing number of parties involved in a cloud environment, authorization is important to ensure the integrity of the data.

3) Availability: This refers to the property of a device that is available and usable by an authorized individual upon request. The availability of the system includes the ability of a system to carry on operations even if certain authorities misbehave [6]. The device has to be able to operate even when there is a security threat to ensure availability. The user of a cloud environment, which is discharged from the requirements of hardware infrastructure, depends on the ubiquitous network available.

2. Existing Security Frame Work

For cloud data centers, the most challenging task is the management of residing data under the protection of the private and confidential sectors. Apply encryption on the storage sector and decryption on the authenticated receiving sector to ensure secure data in cloud storage by using a cryptographic method.

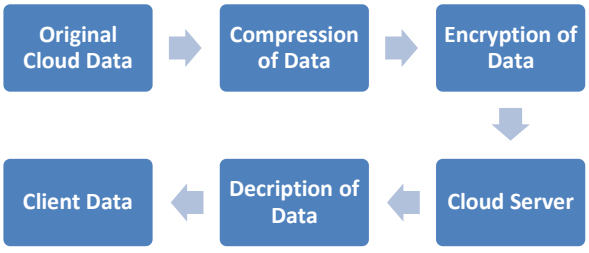

Figure 1. Existing Data Security Model

In most cases, data compression is used to minimize the original size of the data or information, without reducing both its originality and the number of bits.

3. Cloud security challenges

Cloud computing is becoming so popular nowadays that it is in the limelight of the present era. Cloud computing, along with its enormous benefits, poses many security issues that need significant attention to be dealt with in order to improve this technology. These are the main concerns listed below (F, 2014);

- **Outsourcing:** Consumers may lose control when outsourcing the data. It takes some sort of appropriate mechanism to prevent the cloud service provider (CSPs) from using the data against their clients ' consent.
- **Multi tenancy:** Cloud is a shared resource pool. Data protection must be considered when providing the multi-tenant environment.
- **Service Level Agreements:** A specific Consumer-Provider contract is required. The main objective of the agreements is to build the confidence.
- **Heterogeneity:** Different cloud providers have different data protection mechanisms which present challenges for integration.
- **Server Downtime**: Downtime is the time the machine stops reacting to the customer after a failure of some operation. The downtime should be kept to a minimum and power backups should be installed to minimize downtime.
- **Backup:** In case of any service failure, data uploaded by the customers should be backed up. Cloud Seller should mention, in SLAs, what the remedy or solutions to such problems should be in the event of any disaster. There are very small risks of system wide failure such as flooding etc.
- **Data Redundancy**: Data redundancy is a condition in which two different places carry the same data. In the case of cloud computing, it can be understood as providing the clients with copies of the same data, systems or equipment. Cloud vendors should try to keep a minimum of data redundancy.

4. Factors Involved in Cloud Security

Various key factors can affect the efficiency of cloud computing because it is surrounded by various technologies such as load balancing, network, competition control, virtualization, operating system, database, memory management, etc.(Qadiree & M, 2016) Figure 2.

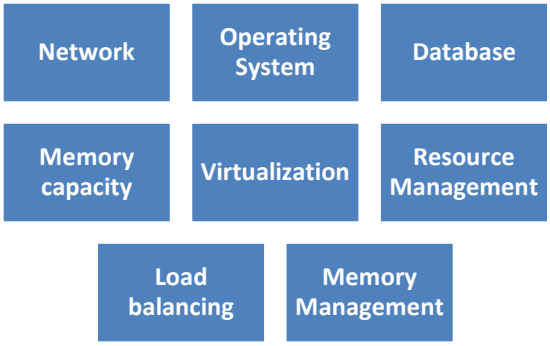

Figure 2 : Technologies involved in cloud computing that can affect the data security

Such technologies ' security factors affecting cloud computing are important, e.g. network that links the cloud computing to the outside world must be secured. The definition of virtualization must be done safely while mapping with the physical systems. Load balancing involves the handling of incoming traffic requests that sometimes overload the server. Algorithms to data mining can be used to deal with malicious attacks.

While cloud computing can be seen as a new phenomenon that is going to revolutionize how we use the Internet, there's a lot to be careful about. Many new technologies are emerging at a rapid rate, each with advances in technology and the potential to make life easier for humans. Several other security issues are present including virtualization security aspects. We assume that attaining end-to-end protection will be difficult due to the complexity of the cloud. The

challenge we face, however, is to maintain more stable operations, even when some parts of the cloud fail.

III. LITERATURE REVIEW

Mohammed Abdelhamid proposed multiple RSA algorithm-based techniques in 2009 to improve the privacy of users. "The author's main purpose is to allow users access to remotely stored data." So that all of the data can be authentically preserved.

In 2010, S Subashini and V Kavitha introduced a complex security architecture using various methods and techniques, Different part provides different security styles. In the year 2010 M. Ahmed et al. described the accuracy of various client-and cloud-related security issues. A main objective is to protect the cloud services and data from the client that are available on the cloud server.

In 2011, V. Krishna Reddy and Dr. L. S. Reddy suggested different level of cloud security architecture. Our main objective is to protect the cloud services and data from the client that are available on the cloud server. We also provide analysis of various types of cloud computing services such as SaaS, Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Syam Kumar P and Subramanian R introduced Elliptical Curvlet Cloud and sobel series for client data protection and cloud resources in 2011. "It uses some set of rules to provide protection and also to abstain from the honesty called data correctness. We also provide protection on the internet against various hackers which may be harmful to our data.

Abbas Amini proposed cloud computing's secure storage system in 2012. They use the algorithm in their paper to maintain data accuracy and to improve security. They used the RSA Algorithm for this purpose. And another algorithm they used is the AES algorithm to keep customer data storage private.

In 2013 Rahmani et al. suggested Encryption as a Service (EaaS) as a solution for cloud computing cryptography based on the concept of XaaS. This approach provides an answer to avoid the security risks of the encryption by the cloud provider and the inefficiency of the encryption on the client side. There is however no comparative study of cryptographic algorithms that can be included in this solution.

In 2014, the cloud computing data storage system protection proposed by SwarnalataBollavarapu and Bharat Gupta for the data of clients. "This system uses different algorithms for encryption & decryption techniques, such as RSA, RC4 and ECC."

In 2015 Velumadhava Rao, K. Selvamaniaddresses various challenges to data security in cloud computing and its solutions. The main purpose of this practical review is to improve data security, so that integrity can be maintained.

Dr. Salim Ali Abbas, Amal Abdul BaqiMaryoosh provided an efficient, flexible and secure method of delivering data and cloud resource security for clients in 2015. They also provide for data correctness and security with the Elliptic Curve Cryptography algorithm.

In 2016 AL-Museelem Waleed, Li Chunlin gave an assessment of how the lack of security affects the data and cloud resources of users. In this, UEC (Ubuntu Enterprise Cloud) is used to solve identity confidentiality issue. The algorithm they've used includes data encryption and decryption to maintain cloud privacy and security integrity.

The first to suggest the use of cryptography to protect cloud computing was Dimitrios et al. Many authors have since proposed using cryptographic algorithms in

the cloud storage. Nevertheless, because they do not specify which algorithm is recommended to encrypt data and how to distribute cryptographic keys while preserving adequacy with cloud characteristics, these solutions remain incomplete

IV. RESULTS AND DISCUSSION

1. Security Problems Faced by Cloud Computing

In terms of privacy and protection, the vulnerability to cloud is strongly influenced. People like providers need to ensure that people who use the cloud do not face a problem like data loss or data theft. There is a possibility of a malicious user or hacker accessing the cloud by impersonating a legit user. The entire cloud affects a lot of people who use the cloud. Some of the challenges that cloud computing faces are:

i. Data theft
ii. Privacy problems
iii. Integrity of data
iv. Infected Applications
v. Loss of data
vi. User level Security
vii. Vendor level Security

The current generation of cloud computing services does not protect the privacy of cloud users and therefore important data such as medical records, financial records or business data are not to be stored. We are engaged in different research projects ranging from theory to implementation in order to address this. Encryption is primarily used to ensure privacy by abstracting all valuable plaintext information. In the sense that the encryption does not access it, it modifies useless data. In order to eliminate this problem we will be developing algorithms for cryptosystems that will allow you to perform a variety of calculations on encrypted cryptographic data, from regular computing use to special computing. Homomorphic cryptography research includes full homomorphic encryption function, searchable encryption, structured encryption, feature encryption.(Chatterjee & Roy, 2017).

2. Cloud computing security: suggested solutions

Several cloud computing scientists have put forward ideas to improve cloud security. Some of these studies are discussed here in addition to their studies. According to the scientists, data should be secured in three major situations: when data move between the user's website and the cloud, in the cloud itself, and during transactions, for instance when a customer has the ability to access information during transaction processing. This analysis includes ensuring that the data are protected and that the provider is assured. However, the client still verify the security issues.

The concept of cloud computing precedes other Internet applications, because of the existence of cloud simplicity. However though such computing improves processing capacity and lowers running costs, a security hazard exists in order to guarantee the information security for the data stored in third parties' areas, in particular in the Internet.

3. Cryptography: Security principles & Algorithms

Cryptography can increase number of privacy related companies to incorporate cloud computing. Cloud computing can help secure storage at the most critical level of privacy. Cryptography is the science of secure storage of messages by turning raw data into unreadable types. Cryptography is known as a set of three algorithms in today's world. The algorithms are symmetric, asymmetric and hazing algorithms. The key challenges in cloud computing are data protection problems, backup data, network traffic, file storage and host security, and cryptography can solve them on its own. Encryption technologies such as Secure HTTP, encrypted VPNs, TLS, and Secure Shell etc. should be used for secure and secure communication between

guest domain and host domain or from hosts to managerial systems. Encryption will help us prevent such exploits like man-in-the middle, spoofed attacks, and session hijacking. Cloud Computing offers customers the ability to store data or run apps with computing facilities or infrastructure. While the advantages of cloud computing are very clear, it presents new security challenges because cloud operators should manipulate data for customers without having to have full confidence. We will try to design basic cryptographic and protocols that are tailored to create a balance between security, efficiency and functionality for cloud computing. Cloud data storage increases the risk of data leakage and does not allow unauthorized users to access it. Data owners cannot have full confidence in cloud data management. Cloud data storage and data processing may expose users ' privacy to parities without unauthorized access by owning data or related entities. Cryptography has been widely used to solve these issues to ensure the security, privacy and trust of data in cloud computing(Nigoti, Jhuria, & Singh, 2013)(Stinson).

V. CONCLUSION

Cloud computing is growing as a new trend and many companies and organizations are moving to the cloud, but many of them are lagging behind due to some security issues. Cloud protection is an overarching principle that removes the drawbacks of major MNC, business and organization adoption of the cloud. A lot of encryption algorithms can be used in the cloud. Some of the symmetrical algorithms and some are asymmetrical algorithm. But for cloud computing, that takes care of data security, the security algorithms that allow the linear search on decrypted data are required. In this area of research, there is a large amount of change. In order to secure the web, cryptography can be used in many ways. Crypto graphing, for example, can be used for monitoring cloud access, maintaining cloud data trust, verifiable computing, approving cloud data and authentication. In addition, Cryptography and ID based Cryptography based in Lattice are two key sectors that provide the security of the cloud data in today's world. There is still much research in this area to be done.

VI. REFERENCES

[1]. H. S. Badr, B. F. Zaitchik, and A. K. Dezfuli, "A tool for hierarchical climate regionalization," Earth Science Informatics, vol. 8, no. 4, pp. 949-958, May 2015.

[2]. I. Panel, C. Change, and P. Ivonne, Climate change 2013: The physical science basis: Working group I contribution to the fifth assessment report of the intergovernmental panel on climate change, Intergovernmental Panel on Climate Change, Ed. Cambridge: Cambridge University Press, 2014.

[3]. D. J. Hand, H. Mannila, P. Smyth, and D. J. H, Principles of data mining (Adaptive computation and machine learning). Cambridge, MA: Bradford Books, 2001.

[4]. K. Abhishek, A. Kumar, R. Ranjan, and S. Kumar, "A rainfall prediction model using artificial neural network," in Control and System Graduate Research Colloquium (ICSGRC), 2012, IEEE, 2012. Online]. Available: 10.1109/ICSGRC.2012.6287140. Accessed: Nov. 6, 2016.

[5]. R. VenkataRamana, B. Krishna, S. R. Kumar, and N. G. Pandey, "Monthly rainfall prediction using Wavelet neural network analysis," Water Resources Management, vol. 27, no. 10, pp. 3697- 3711, Jun. 2013.

[6]. B. Wang et al., "Rethinking Indian monsoon rainfall prediction in the context of recent global warming," Nature Communications, vol. 6, p. 7154, May 2015.

[7]. ZaheerUllah Khan and Maqsood Hayat, “Hourly based climate prediction using data mining techniques by comprising entity demean

algorithm", Middle-East Journal of Scientific Research 21 (8): pp. 1295-1300, 2014.

[8]. Rajesh Kumar, "Decision tree for the weather forecasting", International Journal of Computer Applications (0975 - 8887) vol.2, August 2013.

[9]. D. Gupta and U. Ghose, "A comparative study of classification algorithms for forecasting rainfall," 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Sep. 2015.

[10]. A.Geetha And Dr. G.M.Nasira, "Data Mining for Meteorological Applications: Decision Trees for Modeling Rainfall Prediction", 2014 IEEE International Conference on Computational Intelligence and Computing Research, 18-20 Dec. 2014, Coimbatore, India.

[11]. V. B. Nikam and B. B. Meshram, "Modeling rainfall prediction using data mining method: A Bayesian approach," 2013 Fifth International Conference on Computational Intelligence, Modeling and Simulation, Sep. 2013.

[12]. Gokila, K.Anand Kumar, A.Bharathi, "clustering and classification in support of climatologyto mineweather data-areview", international conference computing and intelligence systems, ISSN: 2278-2397, volume:04, pages: 1336-1340, march 2015.

[13]. EimanTamah A1-Shammari, Mohsen Amirmojahedi,SahaboddinShamshirband,Dalibor Petkovic NenadT.Pavlovic, Hossein Bonakdari, "estimation of wind turbine wakeeffect by adaptive neuro fuzzy approach", flow measurement and instrumentation, volume: 45, PP: 1-6, 2015.

[14]. Oleg V.Diyvankov, Vladimir A.lykov and Serge A.Terekhoff (1992), "Artificial Neural Networks in WeatherForecasting", PP: 829-835, February 1st, 1992(in Russia).

[15]. Gaurav J.Sawale, Dr.Sunil R.Gupta,"Use of Artificial Neural Network in Data Mining for Weather Forecasting", International Journal of Computer Science and Applications, ISSN:0974-1011, vol.6, No.2, PP:383-387,April2013.

Cite this article as :

Rajesh Keshavrao Sadavarte, Dr. G. D. Kurundkar, "Cloud Computing Security using by Applying Cryptography Technique", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 1, pp. 126-132, January-February 2020. Available at doi : https://doi.org/10.32628/CSEIT206123
Journal URL : http://ijsrcseit.com/CSEIT206123