Security Issues in Cloud Computing

A.N. Vaishnavi [#1], R.Anitha [#2]

[1]*Master of Computer Applications, S.A. Engineering college, Chennai-77.*
anvaishnavi3@gmail.com
[2]*Asst Prof., Department of Computer Applications, S.A. Engineering College, Chennai-77.*
anitha@saec.ac.in

Abstract— Cloud computing is the latest of all computing models. It promises to change the way people use computing resources. It gives the opportunity for the people to share resources, services and information among the whole world. IN scientific and industrial area the cloud computing is increasing. With the development of Cloud computing data security is becoming more and more important. Due to data security issues with cloud computing many business organizations have horror in accumulating their information in cloud. This paper cover issues related to secure communication and hiding information from others. So, to ensure the security of data, RSA algorithm has been implemented.

Keywords— Cloud Computing; Security; decryption, RSA algorithm; Encryption

1. Introduction

Cloud Computing is the most significant and mounting idea for both the makers and the users, it is the subsequently big wave in computing. Resources are shared among all the users, servers and individuals. It allows consumers and businesses to use application without installation. There are many benefits in using Cloud computing, like it has better hardware management. As, all the computers are the same and run in the same hardware.

Cloud Computing suggests new services for computing and relates issues like compute, storage, software. Data are not "chained" only in one location; rather, it can be accessed from anywhere and any computer with internet access. In Cloud computing different security, service models and also algorithms are applied. Cloud Service are separated into three types: Software as a Service (SaaS), Platform as a Service (Paas), and Infrastructure as a Service (IaaS).Security problems are Data honesty, Data robbery, Data backup, privacy and many more. In this work RSA algorithm is been implemented before storing the sensitive data in cloud. Computer based security measures capitalizes on user approval and verification.

2. Data Security Issues in the Cloud

However Cloud offers sophisticated storing and access environment, it is not Hundred per cent reliable; the challenge exists in safeguarding the approved access. The secured data trading is important for any network; so it is very important to take safety and privacy into reason when designing and using cloud services.

2.1 Data Confidentiality

Lots of data are stored in the cloud. But there are questions to be replied:

- Will this data remain confidential?
- Will the cloud provider keeps his capacity and not peak into the data?

So, assurances should be provided to the clients and proper performs and privacy policies and actions should be in place to assure the cloud users of the data safety.

2.2 Data integrity

- How to identify if the cloud provider is doing computations correctly?
- How to ensure that the cloud provider didn't Tamper or change data?

2.3 Data Availability

Customer data is usually stock up in chunk on diverse servers often resides in special locations or in dissimilar Clouds. In this case, data accessibility becomes a major legitimate problem as the accessibility of uninterruptible and faultless stipulation becomes relatively hard.

2.4 Data Location and Relocation

Cloud Computing presents a high degree of data mobility. Customers do not always recognize the position of their data. When an venture has some responsive data that is reserved on storage device in the Cloud, consumers desire to identify the site of data and also desire to identify required location. This, then, needs a contractual agreement, between the Cloud provider and the user that data should continue in a fastidious location or exist in on a given recognized server and also, cloud providers should obtain responsibility to make certain the security of systems and offer robust verification to defend customers' information. For instance, emails, photographs uploaded to

Face book can inhabit wherever in the world and Face book members are normally not concerned.

3. Security Challenges in Cloud

Though Cloud gives complicated storage and access atmosphere, it is not hundred per cent dependable; the challenge exists in ensuring the certified access. Because third parties create the choice regarding our data, safety is a big distress. So cloud must make sure that the data entrée is by the trusted users.

Data privacy and auditability topped the list of prime obstacles for the utilize of cloud computing technologies in their associations, according to a current review of over 1100 Indian Business professionals.

4. Base Methodology

The RSA algorithm is the mainly usually used encryption and verification algorithm. clinet data is encrypted first and then it is stock up in the Cloud. When necessary, clinet places a demand for the data for the Cloud provider; Cloud supplier validates the user and delivers the data. It is incorporated as division of the web browser from Microsoft.

4.1 RSA Algorithm Involves Three Steps

- Key Generation
- Encryption
- Decryption

A. Key Generation

Before the data is encrypted, Key generation should be done. This procedure is done among the Cloud service provider and the client.

- Prefer two separate prime numbers a and b. For safety purposes, the integers A and B should be selected at random and should be of comparable bit length.

B. Encryption

Encryption is the method of adapting original plain data into cipher data. Steps:

- Cloud service provider should provide the Public- Key pk to the user who needs to stock up the data with him.
- User data is now planned to an integer by using an decided upon reversible etiquette, known as padding scheme.
- Data is encrypted and the resulting cipher data C is: C = me (mod n).
- This encrypted data is now stock up with the Cloud service provider.

C. Decryption

Decryption is the procedure of changing the cipher data to the original plain data. Steps:

- The cloud client needs the Cloud service provider for the data.
- Cloud service provider confirms the legitimacy of the client and offers the encrypted data i.e., C.
- The Cloud client then decrypts the base by computing, m = Cd .
- Once m is gained, the client can acquire back the unique data by overturning the padding scheme.

5. Conclusion

In this work only the authentic and authoritative client can access the data, even if some unofficial user obtains the data inadvertently or purposely and if captures the data also, client cannot decrypt the data base and obtain back the actual data from it. Data safety is offered by executing RSA algorithm.

References

[1] Zaigham Mahmood, “Data Location and Security Issues in Cloud Computing”, Proceedings of International Conference on Emerging Intelligent Data and Web Technologies, Vol.3,2011, pp.78-92.

[2] Vishwa gupta, Gajendra Singh, Ravindra Gupta, “Advance Cryptography algorithm for improving data security”, International Journal of Advanced Research in Computer, Vol.2, 2012, pp.45-53.

[6] Simarjeet Kaur, “Cryptography and Encryption in Cloud Computing”, VSRD International Journal of Computer Science and Information Technology, Vol.2 (3), 2012 ,pp. 242-249

[7] Aqueel Ahmed A. Jalil, Dr. Santosh S. Lomte and Sanjay Y. Azade, “Cloud Computing Model for Accession of data Through Virtual Computing Lab: An Overview”, International Journal of Linguistics and Computational Applications, Volume 2, Issue 4, October – December 2015, pp.78-83.

[8] Sreela Sreedhar, Varghese Paul and A. S. Aneesh Kumar, “Solitude Conserve Attribute Cryptographic CP-ABFE Data Protocols in Fuzzy Cloud Service Provider”, Indian Journal of Science and Technology, Vol 8(25), 75227, October 2015, pp.1-5.

[9] Birendra Goswani, Dr.S.N.Singh, “Enhancing Security in Cloud computing using Public Key Cryptography with Matrices”, International Journal of Engineering Research and Applications, Vol 2, Issue 4, July-Aug 2012, pp. 339-344.

[10] G.Jai Arul Jose,C.Sanjeev, Dr.C.Suyambulingom, “Implementation of Data Security in Cloud Computing”, International Journal of P2P Network Trends and Technology, Vol 1, Issue 1, 2011, pp.45

Vaishnavi A.N is holding a under graduation degree B.C.A from SSS Jain college for Women’s and pursuing post-graduation in Master of Computer Applications From SA Engineering college .This Paper is part of curriculum covered under in (MC7413) Technical Seminar and Report Writing.