JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 01 , 2020

RSA Data Security Approach in Cloud Computing

Asif Husain
Research Scholar
Shri Satya Sai University of Technology & Medical Sciences,
Sehore(MP)

Akhtar Husain
Associate Professor
Department of Computer Science and Information Technology
MJPRohilkhand University, Bareilly

Abstract— Cloud Computinghas become one of the most important research area because it has the ability to reduce the costs and efforts associated with computing. Now a days, it is most interesting field which offers the services to users on demand over the internet. Due to storing the data and disseminated resources in the open environment, security has become the main concern of Cloud environments. There are many challenges for security of data although Cloud Computing is promising. To ensure the proper security of data, we proposed RSA algorithm method.

Keywords— Cloud Computing, Data Security, RSA algorithm, Encryption, Decryption.

I. INTRODUCTION

In the current era, Cloud Computing is used in many small, medium and large sized companies.In Cloud Computing data security of a cloud in the major concern. Data Security is always one of the most important concern because of the critical nature of cloud computing and the large amounts of complex data it carries.

Every cloud service seeker either an individual or a company should ask the right questions to the cloud provider before hosting their data or applications on the cloud. Prospective cloud providers should let you know; Are they financially sound? Do they have good security policies and procedures in place? Is the infrastructure meant to host your data shared with lots of other users, or will it be segregated by virtualization?

As many companies move their data to the cloud the data undergoes many changes and there are many challenges to overcome. To be effective, cloud data security depends on more than simply applying appropriate data security procedures and countermeasures. Computer based security measures mostly capitalizes on user authorization and authentication.

II. DATA SECURITY ISSUES IN THECLOUD

Privacy and Confidentiality:

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety.

The cloud seeker should be assured that data hosted on the cloud will be confidential.

Data integrity:

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

For compliance purposes, it may be necessary to have exact records as to what data was placed in a public cloud, when it occurred, what virtual memories (VMs) and storage it resided on, and where it was processed. When such data integrity requirements exists, that the origin and custody of data or information must be maintained in order to prevent tampering or to prevent the exposure of data beyond the agreed territories (either between different servers or different networks).

Data location and Relocation:

Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server..

ISSN- 2394-5125 VOL 7, ISSUE 01 , 2020

Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers'information.

Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each others'resources.

Data Availability:

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

Storage, Backup and Recovery:

When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers.

In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.

III. DATASECURITY

Data confidentiality and auditability topped the list of primary obstacles for the use of cloud computing technologies in their organizations, according to a recent survey of over 1100 Indian Business Technology professionals (Fig.1).

Fig. 1.Data Security is Top Adoption Obstacle for Cloud in India

The survey conducted by Saltmarch Intelligence in the third quarter of this year measured perceptions of Business technology professionals including their important challenges in adopting Cloud, the drivers, how their organization's plan to use Cloud, the different stages of adoption, and the cloud platforms, applications, clients, infrastructure and storage used.

Financial savings, agility and elasticity, all enabled through cloud technology, are crucial in a fast paced business world. At the same time security incidents in the Cloud have made clear that this new promising technology comes with complexity and security and privacychallenges.

"While Data confidentiality and auditability (24.5%) topped the list of primary obstacles for the use of cloud computing technologies, performance unpredictability (20.1%) appeared to be another key factor dampening adoption levels". Data transfer bottlenecks (17.5%) and data lock-in (14.3%) were next on the list of factors as reported by respondents.

Information is produced at a rapid rate and more and more openly shared through new and agile collaboration channels that are no longer under our control."

Hence Security of data has become a major concern. When data mobility is at a high level then the risks and issues increase many folds especially when data is transferred to another country with different regulatory framework. High levels of data relocation have negative implications for data security and data protection as well as data availability.

ISSN- 2394-5125 VOL 7, ISSUE 01 , 2020

Thus the main concern with reference to security of data residing in the Cloud is: how to ensure security of data that is *at rest*. Although, consumers know the location of data and there in no data mobility, there are questions relating to its security and confidentiality of it.

No doubt the Cloud Computing area has become larger because of its broad network access and flexibility. But reliability in terms of a safe and secure environment for the personal data and info of the user is still required.

IV. PROPOSEDWORK

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it.

User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider, Cloud provider authenticates the user and delivers thedata.

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Keyonly.

RSA algorithm involves three steps:
1. KeyGeneration
2. Encryption
3. Decryption

Key Generation:

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps:
1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bitlength.
2. Compute n = a *b.
3. Compute Euler's totient function, Ø(n) = (a-1) *(b-1).
4. Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Keyexponent.
5. Now determine d as follows: $d = e^{-1} (\text{mod } Ø(n))$ i.e., d is multiplicate inverse of e modØ(n).
6. d is kept as Private-Keycomponent, so that d * e = 1 modØ(n).
7. The Public-Key consists of modulus n and the public exponent e i.e, (e,n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d,n).

Encryption:

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps:
1. Cloud service provider should give or transmit the Public- Key (n, e) to the user who want to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as paddingscheme.
3. Data is encrypted and the resultant cipher text(data) Cis
$$C = m^e \text{ (mod n)}.$$
4. This cipher text or encrypted data is now stored with the Cloud service provider.

Decryption:

Decryption is the process of converting the cipher text(data) to the original plain text(data).

Steps:
1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verify's the authenticity of the user and gives the encrypted data i.e, C.
3. The Cloud user then decrypts the data bycomputing,
$$m = C^d \text{ (mod n)}.$$
4. Once m is obtained, the user can get back the original data by reversing the paddingscheme.

ISSN- 2394-5125 VOL 7, ISSUE 01 , 2020

V. EXPERIMENTAL RESULTS

In this section, we are taking some sample data end implementing RSA algorithm over it.

Key Generation:

1. We have chosen two distinct prime numbers a=61 and b=53.
2. Compute n=a*b, thus n=61*53 =3233.
3. Compute Euler's totient function,Ø(n)=(a-1)*(b-1), Thus Ø(n)=(61-1)*(53-1) = 60*52 =3120.
4. Chose any integer e, such that $1 < e < 3120$ that is coprime to 3120. Here, we chosee=17.
5. Compute d , $d = e^{-1} (\text{mod} Ø(n))$,
   thus $d=17^{-1} (\text{mod } 3120) = 2753$.
6. Thus the Public-Key is (e, n) = (17, 3233) and the Private- Key is (d, n) = (2753, 3233). This Private-Key is kept secret and it is known only to theuser.

Encryption:

1. The Public-Key (17, 3233) is given by the Cloud service provider to the user who wish to store thedata.
2. Let us consider that the user mapped the data to an integer m=65.
3. Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and theuser.
   $C = 65^{17} (\text{mod } 3233) = 2790$.
4. This encrypted data i.e, cipher text is now stored by the Cloud service provider.

Decryption:

1. When the user requests for the data, Cloud service provider will authenticate the user and delivers the encrypted data (If the user isvalid).
2. The cloud user then decrypts the data bycomputing, $m = C^d (\text{mod } n) = 2790^{2753} (\text{mod } 3233) = 65$.
3. Once the m value is obtained, user will get back the original data.

VI. CONCLUSION

Cloud Computing is still a new and evolving paradigm where computing is regarded as on-demand service. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography.

Science and Software Engineering, Vol 2, Issue 1, Jan 2012.

[5] V. Sandhya, "A Study on Various Security Methods in Cloud Computing", International Journal of Advanced Research in Computer Science, Volume 2,No.6, Nov-Dec 2011.

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

[7] 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, 339-344, July-Aug 2012.

[8]. 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.

[9].William Stallings, "Network Security Essentials Applications and Standards", Third Edition, Pearson Education, 2007.

Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. Hence forth, data security is provided by implementing RSA algorithm.

VII. REFERENCES

[1]. P.Kalpana, "Cloud Computing – Wave of the Future", International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 3, ISSN 2249–071X, June 2012.

[2]. Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari

ISSN- 2394-5125 VOL 7, ISSUE 01 , 2020

Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840,2011.

[3]. Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", Proceedings of International Conference on Emerging Intelligent Data and Web Technologies-2011.

[4] Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance Cryptography algorithm for improving data security", International Journal of Advanced Research in Computer