International Journal of Scientific & Engineering Research Volume 10, Issue 4, April 2019
ISSN 2229-5518.

Secure Data Storage in Cloud Computing using RSA Algorithm

Y. Kiran Kumar, Dr. R. Mahammad Shafi

Abstract-- Cloud Computing is a way to enhance the facility or add capabilities with liveliness without investing in new infrastructure, training new human resources, or licensing latest software. It extends Information Technology's (IT) existing capabilities. In the preceding few years, cloud computing has full-grown from being a promising business concept to one of the fast growing sector of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to raise about just how secure cloud environment it is. Despite of all the build-up surrounding the cloud, enterprise customers are still unwilling to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to outbreak the market. Due to storing data on cloud there is an issue of data security. To ensure the correctness of user's data in the cloud, we recommend an effective mechanism with salient feature of data integrity and confidentiality. This paper projected a mechanism which uses the concept of RSA algorithm to provide better security to the data stored on the cloud.

Index Terms-- RSA Algorithm, Key Generation, Encryption, Decryption, Cryptosystem, Security, Public Key, Private Key

---------- * ----------

1. INTRODUCTION

With virtualization technologies, cloud computing uses more efficient resources. Cloud computing services are growing. They are expected to grow, to expand and expand more in the coming days. Cloud computing has also become a great platform for innovative solutions and entrepreneurs. Such as more businesses offer new cloud solutions and as a new array of services are designed and offered. A physical server can run many virtual machines and operating systems. However, the increase in software and hardware components, the higher the failure of the failures. Cloud Computing has a facility to use computing resources directly from the Internet. A Computing source may be a combination of software or hardware or both, computing resources are released on the Internet in the form of services. A service allows the user to access a computing resource. Services are operated on the remote server and users access to an interface like browser. A user in cloud computing will store data stored on the remote cloud server. Information technologies are taking new waves in accordance with changing civilizations. Computing significantly expanded, made the database more robust.

Cloud Computing detects and briefly say that Cloud Cloud computing services provide client-specific applications and Data storage through dedicated web servers. Storage on a web server is the amount of data stored by the client store as part of the cloud computing. That means there are no data and applications on the client-utilized computer. Only the operating system and the cloud computing service will be the only application. The client will have to access the applications and data to get the cloud servers straight away from cloud servers. Using cloud computing does not have the risk of software, crash, and databases also, the client-utilized device also works faster.

In Cloud computing data are not stored in user's computer but are stored in Cloud storage which is hosted by third parties. Cloud computing environment allows its resources to be shared among servers, users and individuals, in turn files or data that are stored in the Cloud are openly accessible to all. Due to this open accessibility factor, the files or data of an individual can be used by other users of the Cloud as a result attacking treat on data or files become more vulnerable. Once the intruders get access to data, misuse of it possesses a major risk. The intruder may destroy the original data or disrupt the communication also. Apart from files and data Cloud service providers facilitate critical applications whose security requires a lot of attention. One of the common problem occurs in Cloud is that an

International Journal of Scientific & Engineering Research Volume 10, Issue 4, April 2019
ISSN 2229-5518.

individual may not possess the control over the place of data storage. It becomes necessary for a Cloud user to utilize the resource allocation and scheduling facilities provided by the Cloud service provider in turn at the time of processing it becomes essential to protect the data or files of the individuals. To overcome this problem, security in Cloud computing platform should be implemented effectively.

2. CLOUD COMPUTING DEPLOYMENT MODELS

Cloud computing has existed for a long time, offering different kinds of cloud computing solutions is called cloud patterns. Each model has a unique value proposition, which helps the business develop a different line improvement provider and provides the customer service option. Some of the major or popular cloud computing is as follows.

A. *Private Cloud:* This cloud infrastructure is managed by a company or a third party and only maintains the organization's needs. Example is Redmine, which uses its own VMware vCloud installation to extend this system.

B. *Public Cloud:* This cloud infrastructure is available to a large industry group or general public and is owned by the seller who sells cloud services. Redmine Cloud Services Amazon Web Services subscribes.

C. *Community Cloud:* This cloud infrastructure is a shared community that has more than one organization and support similar services. Redmine Educational Consortium, S Cloud is an academic consortium (open source), a member that gives the right to use.

D. *Hybrid Cloud:* This cloud infrastructure has two or more types of clouds listed above to be separate subjects, but the data and applications portability provided by standard technology. Redmine uses Amazon Web Services to handle interface and VMware vCloud for MySQL database system.

3. CLOUD COMPUTING SERVICES

A. *Cloud Services on the Web:* These are the end users who are most fascinated by the users. Online storage solution like Drop box, cloud computing to reach a higher end user. The general term, these services provide one or more web functionality to the end user, like email, word processing, APIs.

B. *Software as a service (SaaS):* SaaS services allow many users to access an application when all of them provide better accessibility and agility. This is called service or application cloud. SaaS services offer specific business functions and business processes that provide specific group capabilities. SaaS provides services that provide cloud computing features, rather than a cloud structure or platform. For example, it offers a scalable application rather than scalability.

C. *Platform as a service (PaaS):* The user configuration under PaaS does not actually use the applications and the facilities provided by the cloud provider. There are cloud storage options available to customers in utility demand in the need for cloud. This model is today's pre-runner operating all the cloud computing model. In this model, it is actually the application, but the end user is the provider. It provides computational resources through a platform developed and hosted by apps and services.

PaaS generally makes use of separate API's to control the behaviour of a server hosting engine to run and reproduce run environments according to user requests. Each provider exposes his API depending on the relevant key capabilities, the application developed for each particular group provider can not be moved to another cloud host, excluding his API depending on the respective key capabilities. There are attempts to extend simple programming designs with cloud capabilities.

International Journal of Scientific & Engineering Research Volume 10, Issue 4, April 2019
ISSN 2229-5518.

Examples of PaaS providers are Force.com, Google App, Windows Azure.

In Cloud computing data are not stored in user's computer but are stored in Cloud storage which is hosted by third parties. Cloud computing environment allows its resources to be shared among servers, users and individuals, in turn files or data that are stored in the Cloud are openly accessible to all. Due to this open accessibility factor, the files or data of an individual can be used by other users of the Cloud as a result attacking treat on data or files become more vulnerable. Once the intruders get access to data, misuse of it possesses a major risk. The intruder may destroy the original data or disrupt the communication also. Apart from files and data Cloud service providers facilitate critical applications whose security requires a lot of attention. One of the common problem occurs in Cloud is that an individual may not possess the control over the place of data storage. It becomes necessary for a Cloud user to utilize the resource allocation and scheduling facilities provided by the Cloud service provider in turn at the time of processing it becomes essential to protect the data or files of the individuals. To overcome this problem, security in Cloud computing platform should be implemented effectively.

4. THE RSA SOLUTION FOR CLOUD SECURITY

The RSA Solution for Cloud Security enables end-user organizations and service providers to visualize the security of their VMware virtualization infrastructure and physical infrastructure from a single console. The solution offers a solid foundation that enables security of VMware environments to be addressed systematically so that organizations can confidently continue their journey to virtualization and cloud computing models.

With RSA, organizations that are deploying virtualization as the foundation for cloud computing can:

1. Take advantage of best-practice security policies and control procedures aligned with VMware guidelines and regulatory requirements.
2. Distribute security policies and control procedures to appropriate users.
3. Continuously monitor, measure, and enforce IT controls in both physical and virtual environments Collect and correlate security and compliance events across the hybrid IT infrastructure.
4. Employ automated workflow for issue prioritization and remediation.
5. Centrally report on the security and compliance posture of the organization
6. Implement a sustainable, coordinated process that can keep pace with the evolving IT landscape and regulatory climate.[11]

5. RSA CRYPTOSYSTEM

A. RSA Key Genration, Encryption, Decryption Process

RSA has been widely used for establishing secure communication channels and for authentication and the identity of service provider over insecure communication medium. The RSA algorithm involves three steps:

1. Key generation,
2. Encryption and
3. Decryption.

Choose two distinct prime numbers p and q.

For security purposes, the integer's p and q should be chosen at random.

Compute n = p q. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, where φ is Euler's totient function.

Choose an integer e such that $1 < e < \varphi(n)$and gcd(e, $\varphi(n)) = 1$; i.e. e and $\varphi(n)$ are co-prime.

e is released as the public key exponent.

Determine d as $d-1 \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

This is more clearly stated as solve for d given $d*e \equiv 1 \pmod{\varphi(n)}$d is kept as the private key exponent.

International Journal of Scientific & Engineering Research Volume 10, Issue 4, April 2019
ISSN 2229-5518.

By construction, d*e ≡ 1 (mod φ(n)). The public key consists of the modulus n and the public (or encryption) exponent e.
The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.
Key Generation: KeyGen(r, s)
Input: Two large primes :r, s
Compute n = r .s
φ (n) = (r - 1)(s - 1)
Choose e such that gcd(e, φ (n)) = 1
Determine d such that e .f ≡ 1 mod φ (n)
Key: public key = (e, n)
secret key= (f, n)
Encryption:
c = me mod n
where c is the cipher text and m is the plain text.
RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product. Given ci = E(mi) = mi e mod n, then (c1 . c2) mod n = (m1 . m2)e mod n
Decryption
Decryption process Recipient does the following:

Uses his private key (d, a, u) to compute m = (v e c) d mod n Where v= u phi-a mod n. Extracts the plaintext from the integer representative m.

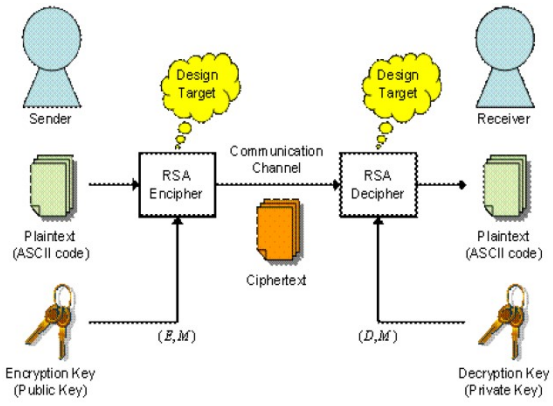

Fig. 1. Encryption and Decryption using RSA

6. RSA IMPLEMENTATION

We divide the program into 3 parts
1. plaintext + publickey1 --> ciphertext1
2. ciphertext1 + publickey2 --> ciphertext 2
3. Cipher text+ private key --> plain text

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.
The keys for the RSA algorithm are generated the following way:
1. n = n1* n2
2. n1 = p x q
3. n = p x q
4. phi = (p – 1) * (q – 1)
5. e = e1*e2
6. Calculate e1 and e2 and multiply two values (e1* e2) or calculate e and divide e into e1 and e2 then we get two encryptions and one decryption.

7. RESULTS:
Key Size: [64]
Generated prime numbers p,q
p: [F764D7D894F53D3B]
q: [B51450AA86BB5BF3]
The public key is the pair (n, E) which will be published.
n:[AEFDEE714CDBE453C43925E72DA61801]
E: [62D89BD8AF5B553E05752479FC024CE3]

The private key is the pair (N, D) which will be kept private.
n: [AEFDEE714CDBE453C43925E72DA61801]
D:[A24C48E0B3CDBF3E3CC5DC3B2CAFC407]

Please enter message (plaintext): This is SECRET iNFORMATION
Ciphertext 1:
[A11029136CC3E9CB2EB63C86C4D2E7E4
6B272C9C065A2BE58D19C338E2FE9689
39EAC1E1C5C738A8E0ECC9A26BC57B45
7F69484A95069014AB62FC638809471B
1AE8A4110F0CF52E88239968892D0A18
39EAC1E1C5C738A8E0ECC9A26BC57B45
7F69484A95069014AB62FC638809471B--]

International Journal of Scientific & Engineering Research Volume 10, Issue 4, April 2019
ISSN 2229-5518.

Ciphertext 2: [2EB448E53B6512572108E04EDE9B9C6
749F0C57F79A4F742A19C49D5662222E
3B1C113EE64666189B324262075F647C
57E1C78D6E55AB018CFAA4B568ACD069
1545023B2083F3DA823D470714AD18B6
3B1C113EE64666189B324262075F647C--]

Recovered plaintext: [This is SECRET
iNFORMATION]

Key Size	Generated Prime Numbers		Generated n-Value	Public Key (Encryption)	Private Key (Decryption)
	p	q			
64	F764D7D894F53D 3B	B51450AA86BB5BF3	AEFDEE714CDBE453 C43925E72DA61801	62D89BD8AF 5B553E057524 79FC024CE3	A24C48E0B3CDBF3 E3CC5DC3B2CAFC4 07
32	A0104A8B	F6B14BCB	9A3E8248CEDCD539	3325C9BF0D4 32609	35500BDF01A5ECE5
16	C047	8095	60936953	216FB57B	59AADC3B

Fig. 2. Public and Private Keys Generation using RSA Algorithm based on Key Size

CONCLUSION

This paper has projected a system to provide integrity, authentication and confidentiality to the data stored in cloud computing. Authentication is achieved because only registered client upload and download the files on the cloud. The RSA scheme used to secure the data in such a way that no leakage of data on cloud could be performed. Always encrypted file stored on the cloud. Thus, in our projected work, only the authorized user can access the data using the generated private key. 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.

This paper discusses the security issues of present cloud computing data security mechanisms and proposes an enhanced data security model for cloud computing to ensure security in each cloud layers. With the help this security model which is RSA Public Key Cryptosystem, we can improve the security flaws of existing data security model in cloud environment and thereby ensuring the data security in cloud environment.

REFERENCES

[1] A. Juels and B. S. Kaliski, Jr., (2007)—Pors: proofs of retrievability for large files," in CCS '07: Proceedings of the 14th ACM conference on Computer and Communications security. New York, NY, USA: ACM, 584–597.

[2] Cody, Brian; Madigan, Justin; MacDonald, Spencer; Hsu, Kenneth W.;, "High speed SOC design for blowfish cryptographic algorithm," Very Large Scale Integration, 2007. VLSI SoC 2007. IFIP International Conference on , vol., no., pp.284-287, 15-17 Oct. 2007.

[3]. 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.

[4]. Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011.

[5]. A. Juels and B. S. Kaliski, Jr., (2007) —Pors: proofs of retrievability for large files," in CCS 07: Proceedings of the 14th ACM conference on Computer and Communications security. New York, NY, USA: ACM, 584–597.

[6]. Cody, Brian; Madigan, Justin; MacDonald, Spencer; Hsu, Kenneth W.;, "High speed SOC design for blowfish cryptographic algorithm," Very Large Scale Integration, 2007. VLSI SoC 2007. IFIP International Conference on , vol., no., pp.284-287, 15-17 Oct. 2007.

[7]. Govinda.K1 Mythili and Geetha Priya(2014),‖ Data Security in Cloud using Blowfish Algorithm‖, International Journal for Scientific Research & Development| Vol. 2, Issue 09.

[8]. A fast implementation of the RSA algorithm using the GNU MP library. By Rajorshi Biswas,Shibdas Bandyopadhyay,Anirban Banerjee, IIIT – Calcutta.

[9]. RSA algorithm using modified subset sum cryptosystem, Sonal Sharma, Computer and Communication Technology (ICCCT), pp-457-461, IEEE 2011.

International Journal of Scientific & Engineering Research Volume 10, Issue 4, April 2019
ISSN 2229-5518.

[10]. Sensitivity of Changing the RSA Parameters on the Complexity and Performance of the Algorithm By Allam Mousa ; Journal of Applied Science 5 (1) :60-63,2005 ISSN 1607 – 8926.Asian Network for Scientific Information.

[11]. RSA SecurBook - RSA Solution for Cloud Security and Compliance