Security Booster for Cloudstash using Modified RSA and Hashing Algorithms

Suman V Chinivar, Arpitha P
Department of Computer Applications
Global Institute of Management Sciences, Bangalore-98

Abstract - Cloud computing is becoming a leading computing model, as all major computing companies are supporting this model and more and more organizations are adopting this archetype.A huge amount of data and programs are storable in clouds. People want to access clouds in various ways. Some access data through monthly memberships, some purchase and some users wants to access data without preserving the data in their devices. For such users, CloudStash provides an enormous opportunity. Thus, security is the major issue that the cloud is facing. Protecting the cloud using normal key management technique opens the risk of attackers hacking the key and confidential data. In the paper, the issues are addressed by proposingmodified RSA and hashing algorithms for CloudStash scheme. Here, the modified RSA algorithm is directly applied on the file. Then we apply hash and sign techniques to provide highly secure cloud by addressing the issues like confidentiality, data integrity, availability and key management.

Keywords - CloudStash, Modified RSA, hashing function

I. INTRODUCTION

Cloud computing is one of the powerful and developing network systems utilized by developers as well as users. Cloud computing allows the data and programs to be shared among servers, users and individuals. In a cloud environment, we can gain access to the applications and data from the remote servers at any time. Cloud computing is growing eventually due to its advantageous cost and also faster access of data.

Cloud holds information about the users which may contain credit card details and even personal information about the users. Since the data and programs are available in the network, accessibility of the data increases; due to which, the attacking threats become more vulnerable in cloud environment. Thus, the data must be protected from the malicious insiders.Encryption is not alone adequate to protect the data;unique techniques have to be used in order to achieve high security. So the issue of privacy and security must be addressed by the cloud providers.

Figure 1: Cloud Stash [3]

People want to access data in various ways. Some access data through monthly memberships; some purchase and download data for offline viewing on their devices; while some others want to purchase data but do not intend to keep it on their devices. For those users who wish to access data without preserving the data in their devices CloudStash provides anenormous opportunity. For example using CloudStash users can purchase a video and it is stored in the cloud and available for them to watch from anywhere, provided the user has the internet connection. Here users can watch or purchase the files from any device that has a browser including tablets,mobile phones and desktops. [1]

Since the data are stored in the cloud, security of the cloud becomes the major concern for all who are associated with the data. Cryptographic algorithms are required which are very efficient and speedily secure the data access.Modified RSA cryptographic algorithms and hashing functions are used to provide security to CloudStash.

Rest of the paper is organized in following manner: In Section II, a literature survey is made on the concept of Modified RSA algorithm and also on Cloud's data security issues and its related work. Meticulous proposed work is offered in section III. Finally Section IV concludes the paper. Section V deals with the future scope on the concept briefed.

II. LITERATURE SURVEY

In RSA algorithm, every alphabet is plotted to another integer. RSA algorithm uses the technique of block cipher where a block of data is encrypted or decrypted at a time. It uses two set of keys: a public-key and a private-key. In the Cloud environment, all the users and the cloud service provider have access to the public-key, on the other hand, users who own the data will have their private-key, which is known only to them. [10].Thus, encryption is done by the Cloud service provider and decryption is done by the cloud user or consumer. At the cloud service providerend, the data is encrypted and stored in the cloud. The cloud user, can access the encrypted data and the user applies his private key and decrypts the data. [10].

RSA algorithms security is based with the integer factorization problem.So, it becomes very crucial task to decide upon the keys. Key selection is the major concern which enhances or which may reduce the security features of the algorithm. The strongest key pair'p' and 'q' to generate modulus n [11] have to be selected carefully.When we have to select two numbers say 'p' and 'q', both the numbers must be large prime numbers which provides high security for the RSA algorithm. Large prime numbers will make it very difficult to apply factorization for 'n' by any known explicit method. All the users know the public-key (e, n).One can try to factorize 'n' and try to deduce 'd'. If small prime numbers are used, it is very easy to deduce 'd'. If large numbers are used, though the effort will be involved in discovering the 'd', but the more amount of time is required to deduce. Thus, selecting the prime numbers is very significant decision in the RSA algorithm. This is the constraint of RSA. The Strength of the cryptographic system of RSA is based on the key size. Also, at the provider and users end, the security key is going to decide the level of security needed. If high level of security is needed, then the chosen prime numbers must be very large. As the prime number size increases, the algorithm will essentially take added time.

Thus, we have used the Modified-RSA algorithm procedure which comprises 'n' distinct prime numbers. So, for all calculations we have used four large prime numbers. There are three components which are comprised in the public key and the private key

Here, for RSA algorithm we take $N = w * x * y * z$,where 'N' is the product of four large prime numbers 'w', 'x', and 'z'. There are three components which make up the public key (e, f, N) where "e" and "f" are chosen randomly. The private key exponent consists of threecomponents (d, g, N). The value of 'N' is kept asboth public and private component. An attacker, who has the knowledge of 'N', still, cannot determine the value of four prime numbers [4].

CloudStash addresses various issues like confidentiality, availability and key management [1].

A. Confidentiality: Confidentiality is achieved by applying modified RSA algorithm on the file. The data isencrypted using the public key bythe cloud service provider. At the user's end, the user is going to decrypt the data using his private key. Since we use four large prime numbers, it becomes very difficult for the hackers to exactly identify each of the prime numbers in the combination.

B.Key Management: Key management deals with the operations for creating, importing, storing, updating, exporting, and deleting the keys [12].Highly secure cloud is based on encryption/decryption of keys that protects the users' data in the cloud [2]. The issues with respect tokey management is how the keys must be stored, the various ways toallocatethe keys between users and the techniques used to protect keys from malicious insiders. Key-Lifecycle Management (KLMS) is a pattern-based method and strict access control to keys and also protected access control procedure for a key-management interface. The enterprise-level key management systems are handled by KLMS. Many endpoints like heterogeneous applications, servers, and network devices to storage devices and mediamight require cryptographic keys which are provided through the KLMS system. The system can provision keys to any application that can receive keys through the Java KeyStore (JKS) interface)[2].

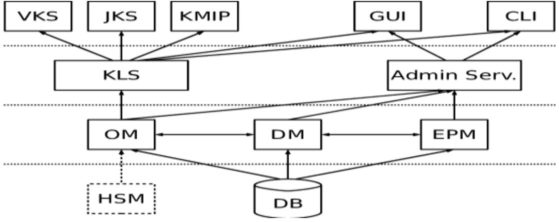


Fig 2: Key Life – Cycle Management Science architecture [2].

C Availability and Integrity: In CloudProof customers cannot only detect violations of write serializability, integrity and freshness;it also proves the occurrence ofinfringement by the third party.[9] CloudProof uses cryptographic tools to allow customers to detect and prove cloud misbehavior. HAIL (High Availability and Integrity Layer) is a distributed cryptographic system that permits a set of servers to prove to a client that a stored file is intact and retrievable [6]. HAIL utilized RAID (Redundant Array of Inexpensive Disk) technique. This technique ensures that the security features such as availability and integrity in intact over multiple clouds.

III. ENCRYPTION AND DECRYPTION

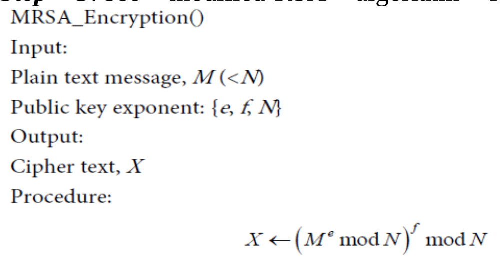
In the paper, for providing high security we have used modified RSA algorithm and hashing techniques.

Algorithm forCloudStash using Modified- RSA algorithm along with hashing.[4]

Step 1: Divide the file into parts.

Step 2:KLMS provides keys to any application that can obtain keys through the Java Key Store.

Step 3:Use modified-RSA algorithm for encryption.


MRSA_Encryption()

Input:

Plain text message, $M\,(<N)$

Public key exponent: $\{e, f, N\}$

Output:

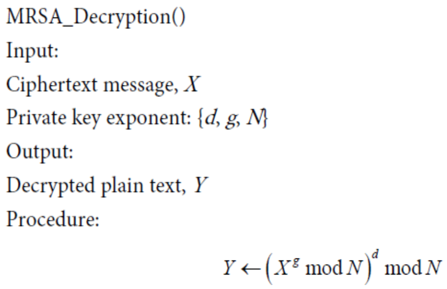
Cipher text, X

Procedure:

$$X \leftarrow \left(M^{e} \bmod N\right)^{f} \bmod N$$

Step 4: For each file do hash and sign.

***Step 5*:**At the users end, the private key is used to decrypt the data that is sent after encryption.



```
MRSA_Decryption()
Input:
Ciphertext message, $X$
Private key exponent: $\{d, g, N\}$
Output:
Decrypted plain text, $Y$
Procedure:
        $Y \leftarrow \left(X^{g} \bmod N\right)^{d} \bmod N$
```

***Step 6*:** Apply the hash on the deciphered data and compare the generated and received signature.

IV. CONCLUSION

Using the combination of modified-RSA and hashing, we get a more secure architecture for CloudStash. Using modified RSA algorithm, it is very difficult for the attacker to deduce the individual prime numbers in the set. This provides increased confidentiality. Using hashing techniques to generate signature, the integrity of the entire cloud is kept intact. Thus, the overall security of the cloud increases making it more preferable to use.

V. FUTURE WORK

In future work, for modified- RSA algorithm the number of prime factorization can be increased to achieve higher degree of security. Elliptical Curve Cryptography can be also implemented in CloudStash which provides the best way of providing data integrity.

VI. REFERENCES

[1]. FahadAlsolami and Terrance Boult, "CloudStash: Using Secret Sharing Scheme to Secure Data, Not Keys, in MultiClouds", 11th International Conference on Information Technology: New Generations, 2014, pp 315-320

[2]. M. Bjorkuvist, C. Cachnin, R. Haas, X.-Y. Hu, A. Kurmus, R. Pawlitzek, and M. Vukolic, “Design and Implementaionof a Key Life Cycle Management System”, in Financial Cryptography and Data Security. Springer, 2010, pp. 160-174.

[3]. Suman V Chinivar, Sirisha G N and Sushma K V, “CloudStash: An Efficient Technique to Provide Security to Multi-Clouds”, in International Journal odf Advanced and Innovative research. Vol no 3, ISBN: 2278-7844.

[4]. Muhammad Ariful Islam, Md. Ashraful Islam, Nazrul Islam, BoishakhiShabnam., “A Modified and Secured RSA Public Key Cryptosystem Based on “n” Prime Numbers”, Journal of Computer and Communications, 2018, 6, 78-90

[5]. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, “Cloud Computing Security: From Single to Multi-Clouds”, 45th Hawaii International Conference on System Sciences, 2012.

[6]. K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16thACM Conf. on Computer and communications security, 2009, pp. 187-198.

[7]. H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10: Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

[8]. C. Cachin R. Haas, and M. Vukolic, “Dependable Storage in the Inter Cloud,” IBM Research, Vol. 3783, pp 1-0, 2010

[9]. R. A. Popa, J.R. Lorch, D. Molnar, H. J. Wang and L. Zhuang, “Enabling Security in Cloud Storage Slas with Cloud Proof,” in Proc. USENIX ATC, 2011

[10]. ParsiKalpana, SudhaSingaraju,”Data Security in Cloud Computing using RSA Algorithm” in International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[11]. Balkees Mohamed, ShereekZaitonMuda, SharifahYasin,”Improve Cloud Computing Security Using RSA Encryption WithFermat’s Little Theorem” in IOSR Journal of Engineering (IOSRJEN) ISSN (e): 2250-3021, ISSN (p): 2278-8719 Vol. 04, Issue 02 (February. 2014), ||V6|| PP 01-08.

[12]. Mathias Bjorkqvist, Christian Cachin, Felix Engelmann, Alessandro Sorniotti. “Scalable key Management for Distributed Cloud Storage”, 2018 IEEE International Conference on Cloud Engineering (IC2E), 2018.