IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Review Paper on Data Integrity for Cloud

Shivani Kaushik[1*], Anirudh Tripathi[2], Pankaj Pratap Singh[3], Amit Kishor[4]

[1]M.Tech Scholar CSE department,Swami Vivekananda Subharti University,Meerut, India
[2,3,4]CSE department, Swami Vivekananda Subharti University, Meerut, India

DOI: https://doi.org/10.26438/ijcse/v7i5.14081411 | Available online at: www.ijcseonline.org

Accepted: 13/May/2019, Published: 31/May/2019

Abstract- Usage of internet applications has increased in this world of technology. Growing technology has both advantages and disadvantages. On the one hand, it provides lots of comfort and ease, on the other hand, it provides it poses a security threat. To secure our communication over the internet we use cryptography. Cryptography is done using asymmetric cryptography and symmetric cryptography.
Asymmetric cryptography uses two keys, one is used for encryption and other is used for decryption. The key used for encryption is public and it is not required to keep it secret. While key used for decryption is always kept secret. In symmetric cryptography both the keys are same and both need to be secret.
RSA is a popular cryptography algorithm. It is an asymmetric-key algorithm. Diffie-Hellman is an algorithm which uses symmetric keys.
This paper presents a novel modified hybrid RSA-Diffie Hellman algorithm, in order to utilize the key benefits of both.

Keywords - decryption, public key, prime number, RSA algorithm, Diffie Hellman algorithm

I. INTRODUCTION

Today's world involves e-commerce and the internet provides a global market place. Instead of running data on a personal device, everything is hosted on cloud storage [13]. We are using cloud computing in our day to day life whether intentionally or unintentionally. Many people don't know that they are using the cloud while using it [11].

Cloud uses network of remote servers hosted on the internet. Cloud stores supervise, and manipulate records, instead of a local server or a personal computer. Using cloud computing, you can access your documents and application all around the world, this helps you to get rid of the limitation of the desktop. There is several security issues related to this technology. This is a common problem when any technology expands. Storing and transferring data on remote server leads to security issues [7].

Quality-of-service management is one of the challenges faced by cloud. While providing services to the customer, it is necessary to avoid hacking of data, especially data of banks and institutions.

Some tamper data for creating trouble to other internet users, while other hack data to obtain the password or other sensitive data of some organization. Data integrity technique protect against loss in the flow of data. There is a lack of security conservation even after so many improvements in technology [2]. Cryptography is a way to hide the data while sending to another user. It is art to hide data from unauthorized user. Due to growing technology, the need for data security has also increased [14]. Since a lot of data is present on the cloud, it includes data which need to be secure.

Authorization of data is checked by the RSA algorithm [1]. To provide the security we use cryptography. Cryptography is used to encrypt and decrypt data. Using cryptography, we can send sensitive data over an insecure network. This helps to avoid unauthorized reader to read it. Cryptography involves encryption and decryption of data. Encryption converts plain text into cipher text. Original data is called plain text and unreadable format of data is called cipher text.
Cryptography is of two types.

1. Asymmetric cryptography (also called as public key cryptography)
2. Symmetric cryptography (also called as private key cryptography).

Hybrid cryptography uses a combination of symmetric and asymmetric cryptography.
Symmetric encryption algorithm uses one key for both encryption and decryption and asymmetric-key uses separate key for encryption and decryption. It helps to successfully exchange secret keys over the public channel [3]. Data

© 2019, IJCSE All Rights Reserved

protection plays an important role in data transmission through the communication channel. Therefore, confidentiality, integrity, and availability are regarded as the key objectives on the topic of data security [6].

To achieve optimal efficiency, both the algorithms are combined together and make a hybrid algorithm. The hybrid algorithm helps to achieve optimal efficiency [11].

In this paper, we are using RSA and Diffie Hellman algorithm. RSA is public key cryptography algorithm and Diffie Hellman is a secret key cryptography algorithm. This hybrid approach is meant to get security advantage of asymmetric key algorithm and speed advantage of the shared key system.

Section 1 contains the abstract. Section 2 contains the introduction in which we are giving a brief description about our review paper. Section 3 contains the related work; in which we have mentioned what we have studied in different sources of material that we have gone through. Section 4 contains a brief comparative study of the two well-known algorithm- RSA and Diffie Hellman. Section 5 contains future work which contains information about our forthcoming research work. Section 6 contains conclusion in which we have explained what we concluded after going through different available study materials. Section 7 contains reference which lists the sources of information used in our review paper.

II. RELATED WORK

2.1 Private Key cryptography -private key cryptography is an encryption method in which the sender and the receiver have the same key. These key represent the shared secret key between parties. This was the only encryption that was in scope of knowledge until June 1976.

The symmetric key is beneficial because: they are inexpensive to produce a strong key. It provides protection of higher level in comparison to the size of the key. The size of the key often small and security provided is high. They are relatively inexpensive to process. It is highly efficient because it does not provide any delay in output as a result of encryption and decryption. It also provides authentication because encryption and decryption are to be carried out with the same key i.e. the key which is used for encryption is to use for decryption. Thus as long as the symmetric key is kept confidential by both the communicating parties can be sure that they are in communication with the authenticated party [8].

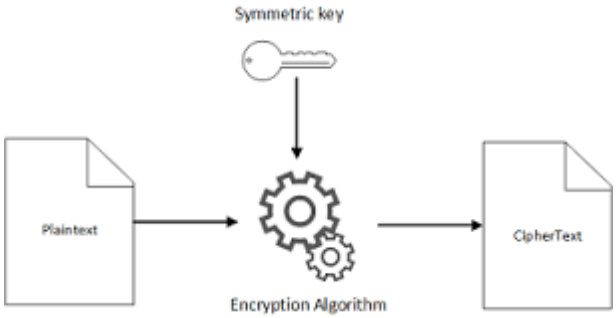

Fig 1. Symmetric key encryption process [11]

In our research paper, we are using Diffie Hellman algorithm. It is a symmetric key algorithm.

Diffie Hellman

This algorithm uses a shared secret key between the two parties. Ralph Merkle gave the idea of this algorithm. This algorithm was named after Martin Hellman and Whitfield Diffie. Diffie Hellman has been used in the field of cryptography since a long time. It secures a variety of services over the internet. It requires an exchange of Diffie Hellman keys over the secure channel. Diffie Hellman is used by protocols like Secure Shell, Secure Sockets Layer and Internet Protocol Security.

The algorithm is as follows:

1. Select two number 'G ' and prime number 'R'.
2. Select a number 'A' and another number 'B', both A and B are to be kept secret.
3. Calculate number $X=G^{\wedge A}$ mod R, and $Y=G^{\wedge B}$ mod R. These X and Y are to be kept as public key.
4. Interchange these public numbers.
5. Compute initial key as KA, KA=Y^A mod R and
6. Compute other key as KB, KB KB= X^B mod R
7. Here KA= KA=K. [12]

2.2Asymmetric cryptography -

It is cryptography which involves two keys. These two keys are public key and private key. The public is to be distributed. It may be given to trusted or untrusted. But private key needs to be kept confidential just like in case of symmetric key cryptography. Neither key will do both the functions.

Asymmetric cryptography has two primary use cases: authentication and confidentiality. Using asymmetric cryptography, messages can be signed with a private key, and then anyone with the public key can verify that the concerned message was created by someone possessing the corresponding private key. This can be combined with a proof of identity system to know what entity (person or group) actually owns that private key, providing authentication.

The private key is used for decryption of the message while the public key is used for encryption of message

© 2019, IJCSE All Rights Reserved

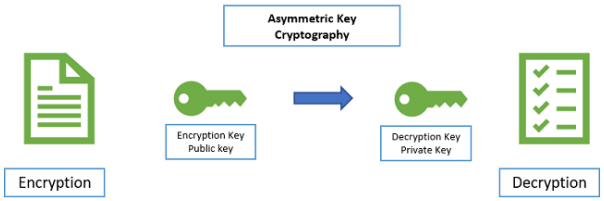

Fig 2. Asymmetric key cryptography

Many protocols like SSL/TLS, S/MIME, SSH, and OpenPGP use asymmetric cryptography for encryption purpose. Encryption strength is directly related to key size and doubling key length delivers an exponential increase in strength, although it impairs performance. As computing power enhances and more efficient factoring algorithms are discovered, the ability to factor larger numbers also increases [4].
In our research work, we are using RSA algorithm.

RSA algorithm:
RSA consist of two keys. Encryption is done by public key and decryption is done by private key. The security offered by RSA algorithm is dependent on the factorization of the integer problem. So the key selection is crucial in RSA. It takes two prime numbers and multiplies and applies some additional operation on it and generates two sets of keys. If anyone knows the factors after multiplying two prime numbers, then encryption can easily break. [5]
RSA algorithm steps are as follows:
1. Assume two prime numbers p, and q, of an approximately equal size such that their product n=p*q is of the required bit length, for
2. Calculate n=p*q and z= (p-1) *(q-1)
3. Assume an integer E, 1<E<z, such that gcd (E, z) =1.
4. Calculate the exponent d, 1<d<z, such that Ed=1 (mod phi).
5. We get (n, e) as public key and (n, d) as private key. Keep all the values d, p, q and z confidential.
Sender side encryption works as follows:
Sender A performs the following steps-

1. Acquire public key (n, e) of receiver B.
2. The plaintext message is represented as a positive integer m.
3. Calculates the cipher text c to b.
4. Cipher text c is sent to B.

Receiver side decryption is as follows:
Receiver b now performs the following steps:

1. Makes use of his private key i.e. (n, d) to calculate $m=c^d \bmod n$.
2. From representative message m, obtains the plain text.

Number theory behind the RSA:
1. Prime number generation is easy- It easy to assume a random prime number of a given size.
2. Multiplication is easy - given p and q, it's easy to find their product, n=p*q.
3. Factoring is hard- given such an n, it appears to be quite hard to regain the prime factors p and q.
4. Modular exponentiation is easy - given n, m, and e, it's easy to compute $c= m^e \bmod n$.
5. Modular root extraction, the reverse of modular exponentiation is easy
6. Modular root extraction is otherwise hard - given only n, e, and c, but not the prime factors, it appears to be quite hard to recover the value m. [9]

III. COMPARATIVE STUDY OF RSA AND DIFFIE HELLMAN ALGORITHM

In this section we are comparing RSA and Diffie Hellman based on certain parameters:

parameters	**RSA**	**Diffie Hellman**
keys	Generating keys for RSA algorithm is extremely difficult.	Generating keys for Diffie Hellman is easy.
security	Relies on the difficulty of integer factorization	Relies on the complexity of the discrete logarithm
Encryption	Encryption is cheaper	Encryption is expensive
Public key encoding	Smaller to encode	Bigger to encode
strength	RSA 1024 bits is less robust than Diffie Hellman	Diffie Hellman 1024 is much more robust
authentication	Authentication only sender	Authenticates both sender and receiver
attacks	Susceptible to low exponent, common modulus and cycle attack	Susceptible to the man in the middle attack.

[8]

IV. FUTURE WORK

After studying both the RSA and Diffie Hellman algorithm deeply, we have realized that there is scope of improvement. We will further carry on research on this topic. We will improve the hybrid RSA Diffie Hellman algorithm by reducing the time consumption of the algorithm and increasing the security of the algorithm.

© 2019, IJCSE All Rights Reserved

V. CONCLUSION

Data security and data integrity are major issues of today's world of growing technology. After research across available techniques and available techniques and material, it is found that there is still a need for improvement. Keeping in mind security issues and time-issues we are working on a hybrid of two of the best algorithm RSA and Diffie Hellman.

After studying the RSA and Diffie Hellman algorithm we have concluded that there is a security issue. There lies a threat of data loss; data tamper etc. besides there is also an issue of time consumption. So we are trying to solve both the issues.

In this paper, we are working on how to decrease encryption-decryption time and improving hybrid RSA Diffie- Hellman algorithm. Encryption and decryption is done by RSA while key generation is done by diffie Hellman. Benefits of both the algorithm are utilized in hybrid algorithm RSA algorithm has a security issue. Though it offers a high level of security, still, there is always a security threat. Besides this, there is always a requirement of less time taking algorithm. To overcome both these issues we have worked on hybrid RSA Diffie Hellman algorithm. This algorithm provides higher security, as well as this, is less time taking. Providing higher security and taking less time is the demand of the high technology world. Our hybrid RSA Diffie-Hellman algorithm optimizes the benefit of individual algorithm and is suitable for technology-dependent world.

REFERENCES

[1] Mahalakshmi and Suseendran G., (2018). "An analysis of Cloud Computing issues on data Integrity, privacy, and its current solutions".

[2] K David Raju, L Vijay Kumar, K Anthony Rahul Showry, B LhoitKrishn ,(2018) ." techniques of providing data integrity in cloud computing".

[3] Joseph Selvanayagam1, Akash Singh2, Joans Michael3, Jaya Jeswani4 (2018) ."secure file storage on cloud using cryptography".

[4]https://searchsecurity.techtarget.com/definition/asymmetric-cryptography

[5] Shreen Nisha, Mohammed Farik (2017), " RSA public key cryptography algorithm - a review", international journal of scientific and technology research volume 6.

[6] Prabhat Kumar Panda, (2017). "A hybrid security algorithm for RSA cryptosystem".

[7] Sultan Aldossary, William Allen, (2016). "Data Security, Privacy, Availability, and Integrity in Cloud Computing: Issues and Current Solutions".

[8] Ayan Roy (2016)," brief comparison of RSA and Diffie-hellman (public key) algorithm"

[9] Israt Jahan, Mohammad Asif, Liton Jude Rozario (2015), Improved RSA cryptosystem based on the study of number theory and public key cryptosystems. American Journal of Engineering research.

[10]https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gtps7/s7symm.html

[11] Miss. Renushree Bodkhe , Prof. Vimla Jethani , (2015) "Hybrid encryption algorithm based improved RSA and Diffie - Hellman ".

[12] Gaurav R. Patel, Prof. Krunal Panchal (2014), "Hybrid encryption Algorithm".

[13] Mahima Joshi, Yudhveer Singh Moudgil,"secure Cloud Storage."

[14]Sarthak R Patel, Prof. Khushbu Shah, Gaurav R Patel, "Study on Improvements in RSA algorithm"

[15] P. Anusha, . R. Maruthi " A survey paper on data integrity for cloud"

[16] Shraddha Saxena , Manish Sharma "Secure technique to achieve data privacy and data integrity in cloud computing "

Authors' Profile

Shivani Kaushik is pursuing M. Tech. from Subharti Institute of Engineering and Technology, Swami Vivekananda Subharti University, Meerut, India. She received her B. Tech Degree in computer science and Engineering from Uttar Pradesh Technical university, Lucknow, India. Her area of interest is cryptography.

Er. Anirudh Tripathi is working as Assistant Professor in the department of Computer Science Engineering and I.T., Subharti Institute of Engineering and Technology, Swami Vivekananda Subharti University, Meerut, India.

Er. Pankaj Pratap Singh received his B. Tech Degree in Computer Science Engineering from Uttar Pradesh Technical University, Lucknow, India, in 2007 and M. Tech degree in Medical Image and Image Processing from Indian Institute of Technology Kharagpur, Kharagpur, India, in 2010. He is currently working as Assistant Professor in the Department of Computer Science Engineering and Information technology, Subharti Institute of Engineering and Technology, Swami Vivekananda Subharti University, Meerut, India. His research interests include IOT, Neural Network, Machine Learning, Deep Learning, Image Processing techniques, Cognitive Science, Computer Network and Data Mining techniques.

Er. Amit Kishor is working as Assistants Professor in the department of Computer Science Engineering and I.T., Subharti Institute of Engineering and Technology, Swami Vivekananda Subharti University, Meerut, India. Currently he is pursuing Ph. D. in Computer Engineering from Department of Computer Science and I.T., Sam Higginbottom University of Agriculture, Technology and Sciences, Allahabad.

© 2019, IJCSE All Rights Reserved