7th National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(1st and 2nd March 2019)
International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

Securing Files on Cloud through Hybrid Cryptography

Kuldeep Yadav[1], Naveen Yadav[2], Rajnath Yadav[3], Dnyaneshwar Bhabad[4]

Department of Computer Engineering, Mumbai University, INDIA

Abstract**—***Cloud computing is an important application for storage of data on the cloud. Cloud computing platform avoid the burden of local data storage and also reduce maintenance cost it also provides users to access their data whenever they want. Cloud computing is the revolution through which individual can share resources services and data among the users through the network. Since millions of users use the same network for data transfer the data becomes more vulnerable to different security attacks from the intruders. In cloud storage data is move to a remotely located cloud server on which user does not have any control. In cloud computing they are only concerned on providing the security of the data which is stored on cloud but they do not provide security to the data while it is getting transferred. Hence to overcome the drawback of existing system a model which uses hybrid encryption and decryption process based on AES and ECC algorithm can be used. Furthermore, HMAC algorithm is used to ensure the integrity and authenticity of the data. With this system user will get to know if his data is being manipulated or no. By using hybrid algorithm user will get extra security, confidentiality and integrity of data.*

***Keywords—Advance Encryption Standard, Elliptic Curve Cryptography,Hash Message Authentication Code, Public Key Cryptography*.**

I. INTRODUCTION

Cloud Computing provides sharing of resources and services via Internet. In past few years, usage of internet is increasing very rapidly which increases cost of hardware and software. So, this new technique known as cloud computing used to solve these problems by giving service when user demand over the internet and definitely it decreases the cost of hardware and software. Services offered in cloud computing have various features like high scalability, reliability, availability, flexibility and dynamic property. Cloud computing has become a familiar term and most used technology around the world. Client can retrieve data from cloud on request of user. To store data on cloud users, have to face many issues like it could get hacked while transferring or might get manipulated on cloud server. To provide the solution to these issues there are number of ways. Cryptography and steganography techniques are very popular now a day's for data security. Use of a single algorithm is not effective for high level security of data in cloud computing. Hence using hybrid cryptographic algorithms for storage and transfer of data is very useful for providing security to user's data. Using hybrid cryptographic algorithm like AES and ECC provides better security to the users. Cloud storage issues are solved using cryptography techniques. Data integrity is accomplished using SHA1 hash algorithm. Data integrity means user can check data accuracy and consistency of data.

II. LITERATURE SURVEY

2.1 Enhancing the Data Security in Cloud by Implementing Hybrid of Aes and Rsa [1].

This paper has proposed a system on Hybrid (RSA & AES) encryption algorithm to safeguard data security in Cloud. Security and data privacy being the most important factor in cloud computing. This paper mainly focuses on the following key tasks are secure upload of data, secure download of data, proper usage and sharing of public, private and secret keys which are involved for encryption and decryption. They have used key generation technique used in this paper is unique in its own way. This has helped in avoiding any chances of repeated or redundant key. The biggest advantage it provides users the keys which are generated on the basis of system time and so no intruder can even guess them so this increases the security. The main purpose behind using AES and RSA encryption algorithm is that it provides three keys i.e. public key for encryption, and private key and secret key for decryption. The data after uploading is stored in an encrypted form and can be only decrypted by the private key and the secret key which is only known by the user.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

2.2 A Hybrid Encryption Algorithm Based on RSA and Deffie-Hellman [2].

Here they have given information on hybrid of RSA and Deffie-Hellman algorithm. This both algorithms are asymmetric algorithm and they have focused on combining these two algorithms RSA and Deffie-Hellman in order to achieve more security. RSA algorithm is a public key cryptography method. It is widely used in electronic commerce protocol. It has a public key and private–key. This public key is known to everyone and used for encryption and Private Key is used for decryption. These both algorithms use the theory of Prime Numbers. Security of the algorithm is based on the difficulty of factoring large integers. It is the world's most popular asymmetric key Encryption algorithm. In this approach the Deffie-Hellman is not only a key generation but also for the generation of cipher text. Generation of prime number for Deffie-Hellman is not easy, so to guess that number of keys is impossible.

2.3 Study on Improvements in RSA Algorithm and Its Implementation [3]

This paper has implemented a system on the Network Security means to protect data during transmission over channel of networks. Cryptography is the way of hiding information during transmission over a communication cannel. There are lots of cryptographic algorithms available to protect user's data from intruders. RSA is an effective algorithm which provide security and uses the public key cryptographic which needs time and memory for key generation. The performance of RSA will be improved by reducing the modulus and private exponents. Using RSA algorithm and DES key for data transmission, so it is no need to transfer DES key secretly before communication. Using RSA to send keys, so it can also be used as digital signature.. RSA variants which can improve the performance of the decryption and signature. The performance of RSA will be improved by reducing the modulus and private exponents. At the same time, it will get higher security and higher speedup based on current devices.

2.4 A Hybrid Security Approach Based on AES and RSA for Cloud Data [4].

They have implemented an efficient and secure cloud computing framework which support security for the cloud users and data control is being provided at the cloud user side. The cloud user can use the privilege of inter cloud communication with the data security of AES and RSA algorithms. The hybridization which will provide four key security. The encryption is provided by the server. If any malicious behavior is identified before the cloud user read operation then client document identification bit alerts the client and server for the possible attack. It provides security with two standard encryption mechanisms namely AES and RSA. They have designed a secure user cloud framework with the help of AES and RSA algorithms approach provides an authenticated way of entering the cloud user and provides inter cloud communication virtualization environment. Then they have provided the data identification bit control for controlling any malicious behavior detection.

2.5 Comparison of ECC and RSA Algorithm in Resource Constrained Devices [5].

This paper gives description about ECC and RSA algorithm. The usage of resource constrained devices is increasing these devices primarily working with sensitive data. This study will compare elliptic curve cryptography algorithm with key size of 160 bit and RSA algorithm with key size of 1024 bit. RSA and ECC are known as the most efficient among all asymmetric encryption algorithms. The bigger the key size is the more secure the algorithm is. But in the other hand, bigger key size requires more computational power and resources and rationally these prerequisites will lower the algorithm's performance. Performance of an ECC algorithm depends on efficient computation of scalar multiplication (kp). Key size of 160-bit ECC has equivalent security level with 1024-bit RSA algorithm. Observed that RSA security required 1024 bits for corporate use and 2048 bits for extremely valuable keys. Therefore, the advantage of ECC over RSA is obvious since with a shorter length for key it can provide the same level of security as RSA.

2.6 A Survey Paper on Elliptic Curve Cryptography [6]

In the proposed system information about Elliptical curve cryptography (ECC) which is based on a public key cryptosystem. Elliptic curve cryptography can be used to create smaller, fasters, and more efficient cryptographic keys. ECC authentication schemes is more suited for wireless communications, like mobile phones and smart cards, personal information like financial

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

transaction or some secrets medical reports, confidential data where main considerations is to provide secure data. Elliptic curve cryptography (ECC) system is used to provide suitable authentication RFID system because it can provide similar security level but using a smaller key sizes and has low computational systems needs. The low processing associated with ECC authentication schemes is to make appropriate for use with RFID tags because they have consuming limited computing power. They have presented a survey on ECC based RFID authentication scheme that is suitable for many applications where security is main concern. The smaller key sizes makes faster cryptographic operations, running on smaller chip and on more compact software.

2.7 Research Issues on Elliptical Curve Cryptography and Its Application [7].

This paper has proposed system on the different applications and advantages of ECC algorithm over different algorithms and they have also made a comparison between RSA and ECC algorithm. ECC offer equals security for a far smaller key sizes, thereby reducing processing overhead. ECC is a kind of public key cryptosystems like RSA. But it differs from RSA in its quicker evolving capacity and by providing attractive and alternate way to researchers of cryptographic algorithm. The security levels which is given by RSA, can be provided even by smaller keys of ECC. For example, the 1024-bit security strength of an RSA could be offered by 163-bit security strength of ECC. Other than this, ECC is particularly good for wireless communications, like mobile phones, PDAs, smart cards and sensor networks. ECC point of multiplication operations is found to be computationally more efficient than RSA exponentiations. ECC offers considerably greater security for a given key size.

2.8 Enhanced Cloud Data Security Using AES Algorithm [8].

This paper has proposed system on the importance of cloud computing providing security to these data has become the critical area of concern. The current system for data security concentrates on providing security to the stored data in cloud storage but concerns less on securing the data while it is being transferred. The data becomes prone to intruder attacks while being transferred. Also, in the current existing trend, the third-party auditor is given access to data during data transfer. This also increases the access vulnerability of data as the intruder could act as third party and gain access to the data. Considering security as a crucial issue, the system proposed concentrates on providing security to transferring data using encryption technique. The system also takes into consideration the issue concerned with the third-party auditor, that in the proposed approach, the auditor is denied access to the user data. Providing secure data to the users includes providing security during data transfer and the data storage.

2.9 Comparative Analysis of RSA and ECC Algorithm [9].

This paper has shown the comparative analysis of Rives-Shamir adleman (RSA) and Elliptic Curve cryptography (ECC). Cryptosystems based on elliptic curves occur as an alternate to the RSA cryptosystems. The security of the RSA cryptosystem is based on the integer factorization problems (IFP) where as the security of ECC is based on the elliptic curves discrete logarithm problems (ECDLP).This analysis suggests that ECC takes less memory than RSA and is better than RSA, especially on memory-constrained devices. Symmetric-key cryptosystems are encryptions/decryptions systems which provide messages confidentiality only. An asymmetric-key cryptography technique provides confidentiality, integrity, and authentication of travelling or storage message.

2.10 Performance Based Comparison Study of RSA and Elliptic Curve Cryptography [10].

This paper has told about the comparison of ECC and RSA algorithm. Security often requires that data to be kept in safe from unauthorized access and they used in defense physical security (placing the machine to be protected behind physical walls). However, physical security is not permanently an option (due to cost and/or efficiency considerations). Most of computers are interconnected with each other openly, thereby exposing them and the communications channels that they use. Thus, arises the problem of Network Security. It is basically a combinations of an Encrypting systems, and a Decrypting systems. Cryptosystem have been in use all over the world for centuries.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

2.11 Data Security in Cloud Using RSA [11].

They have given us information on different services offered in the Internet as a traditional hosting system. But in the traditional hosting system storage and usage are fixed. But the current trend in business requires dynamism in computing and data storage. They have used RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, Cloud users are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required, user request for the data for the Cloud provider, Cloud provider authenticates the user and delivers the data. RSA is a block ciphers in which every message is mapped to an integer. RSA consists of Public -Key and Private-Key. In the 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 providers and decryption is done by the Cloud user or consumers.

2.12 Elliptic Curve Cryptography for Securing Cloud Computing Application [12].

This paper has explained that computing application and data are growing so rapidly that increasingly larger servers and data center are needed for fast processing within the required time. A fundamental information technology and computing services are being delivered. The out of control cost of power in terms of electricity generation, personal hardware and limited spaces in data center have encouraged a significant number of enterprises to move more infrastructure into a third party provide cloud. This security scheme addresses authentication, authorization, confidentiality, integrity and non-repudiation issues. In ECC cryptography is helps to increase the speed of encryption and decryption and shortening the CPU execution cycle. The algorithm relies on a mathematical problem that is more difficult for hackers to attacks than the current encryptions, it can offer equivalent security with substantially smaller key sizes.

III. ANALYSIS TABLE

The following Table-1 gives the analysis of literature papers on Securing files on cloud through various algorithms. This papers gives a detail explanation of the advantages and disadvantages of the different algorithms. It also tells us about the drawback in the existing systems.

TABLE 1

S. No	Title of Paper	Techniques	Advantages	Disadvantages
1.	Enhancing the data security in cloud by implementing hybrid of Advanced Encryption System and Rivest Shamir Adleman algorithm [1]	Advanced Encryption standard- Rivest Shamir Adleman encryption algorithm.	It is helped in avoiding any chances or repeated or redundant key. Integrity should be maintained.	The problem this paper is they have used less bit key.
2.	A hybrid encryption algorithm based on Rivest Shamir Adleman And Deffie Hellmanm[2]	Hybrid encryption of Rivest Shamir Adleman and Deffie Hellman algorithm.	Security of RSA algorithm was increased further. Key Exchange algorithm.	Deffie Hellman algorithm is a key exchange algorithm hence it cannot be used for encryption and decryption.
3.	Study on improvement in Rivest Shamir Adleman algorithm and its implementation [3]	Data Encryption Standard (DES) algorithm, Rivest Shamir Adleman(RSA) algorithm.	Rivest shamir Adleman Algorithm Used for encryption of the key of DES Because its Management advantages in key cipher.	DES is weak against brute force attack even triple DES. DES has a weak key.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

4.	A hybrid security approach based on Advanced Encryption System and Rivest Shamir Adleman for cloud data [4]	Advanced Encryption system based Rivest Shamir Adleman algorithm.	A hybrid security approach based on Advanced Encryption System and Rivest Shamir Adleman for cloud data.	Data integrity was not provided.
5.	Comparison of elliptic curve Cryptography and Rivest Shamir Adleman algorithm in resource constrained device [5]	Elliptic curve Cryptography and RSA algorithm	A 256-bit key in ECC offers about the same security as 3072-bit key using RSA.	Bigger key size requires more Computational power and resources.
6.	A survey paper on Elliptical Curve Cryptography [6]	Elliptical curve cryptography algorithm.	It can create faster and more efficient cryptography key. Less power consumption and heat production.	ECC algorithm is more complex and more difficult to implement than RSA
7.	Research Issues on Elliptic Curve Cryptography and its application [7]	Elliptical Curve Cryptography algorithm.	It is uses smaller keys to provide high security, high speed in low bandwidth.	RSA uses larger key size as compare to ECC offers equal security.
8.	Enhanced cloud data security using AES algorithm [8]	Advanced Encryption Standard algorithm (Symmetric Algorithm).	Encryption is fast. More secure than DES, 3DES. AES is faster in both hardware and software.	One key. It is exposes user data to a third-party Auditor and is concerned only with security of stored data.
9.	Comparative analysis Of Rivest Shamir Adleman and Elliptical Curve Cryptography [9]	Rivest Shamir Adleman and Elliptical Curve cryptography technique.	ECC takes less time for encryption and decryption. It is also provide key of smaller size as compare to RSA.	RSA takes large time for encryption and decryption as compare to ECC.
10.	Performance Based Comparison Study of RSA [10]	Rivest Shamir Adleman is used.	RSA is more secure it may be stronger by applying some technique.	The attacker can used modulus operator to break the RSA algorithm.
11	Data security in cloud using RSA [11]	Rivest Shamir Adleman.	As it is Asymmetric algorithm it provides better security.	Two keys are used hence encryption and decryption of data takes time.
12.	Secure algorithm for cloud computing and its application [12]	Advanced Encryption system- Rivest Shamir Adleman encryption algorithm.	It is efficient in terms of brute force attack, timing attack and mathematical attacks.	Problem with Distributing key as It shares secret key between only two users.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

IV. PROPOSED SYSTEM

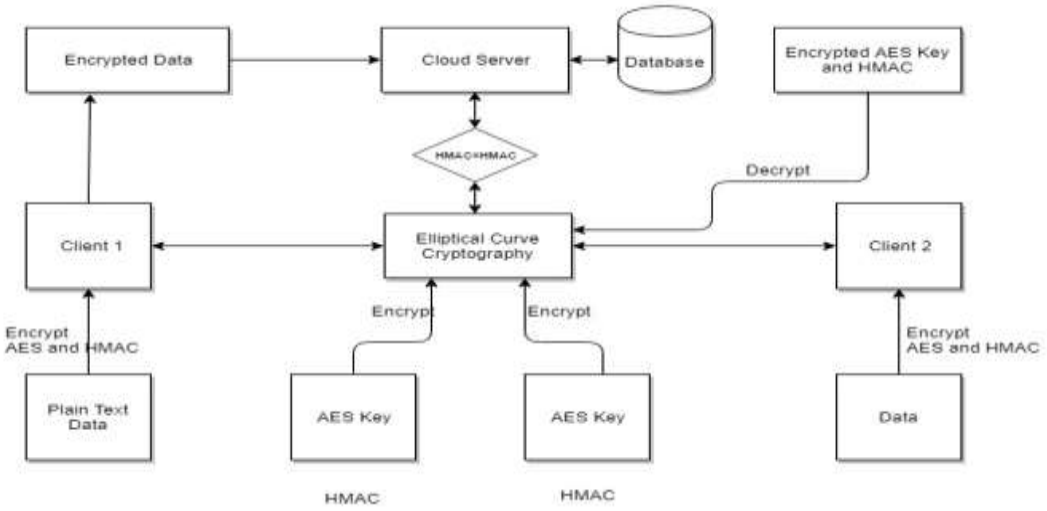

FIGURE 1: System Flow Diagram

The above system flow diagram tells us about how the clients are communicating uploading and encrypting the files on cloud in a secure way. The client 1 has some data which he wants to store on cloud he will first encrypt it using AES algorithm and he will remove HMAC of that data. Then he will store the encrypted data plus hash function to the cloud server. Now if client 1 wants that client 2 should access his data that is stored on cloud then he has to send the AES keys to client 2.

Client 1 will encrypt the AES keys and HMAC using ECC algorithm and he will send it to client 2. Now client 2 has the encrypted keys and HMAC value that client 1 has sent. He will decrypt the keys using ECC algorithm and will check whether the hash function that client 1 has sent and that is present on cloud server are same. If it is same then only client 2 will access the data otherwise, he will directly reject it.

V. CONCLUSION

This system will provide facility to the client by giving proof of integrity of the data which he wishes to store in the cloud storage. By doing this client can get advantage with respect to the cost and efforts. The Purpose of the scheme is to reduce computational and storage overhead at the user side and as well as reduce overhead of the cloud storage server. The purpose is also to reduce network bandwidth consumption. At the user side there are two functions first is bit generator and second is function which is used for encrypting the data. So therefore, as compare to all other scheme this system provides minimal storage at the user side. The scheme is suitable for small memory device like mobile phone. Large computational power is reduced because of encryption of file. As everything is handled through cloud user gets the facility of accessing the data any time he wants. This system will help users to get as surity of their data and will place their trust in using cloud computing and cloud services.

REFERENCES

[1]. V.S Mahalle and A.K Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (RSA & AES) Encryption Algorithm",IEEE,2014, p 146-149.

[2]. S. Gupta and J. Sharma, "A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman ", IEEE 2012.

[3]. P. Saveetha and S. Arumugam," Study on Improvement in RSA Algorithm and its Implementation", International Journal of Computer & Communication Technology, Volume-3, Issue-6, 7, 8, 2012, p 61-66.

[4]. B. Kumar, J. Boaddh and L. Mahawar, "A hybrid Security Approach based on AES and RSA for Cloud Data", International Journal of Advanced Technology and Engineering Exploration, Vol 3(17) 2016, p 43-49.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

[5]. M. Bafandehkar, S. M. Yasin, R. Mahmod, Z. MohdHanapi," Comparison of ECC and RSA Algorithm in Resource Constrained Devices", IEEE, 2013.

[6]. H. Agrawal, P. R. Badadapure, "A Survey Paper on Elliptic Curve Cryptography",Volume: 03 Issue: 04 ,IRJET-2016,p 2014-2018.

[7]. R. Shanmugalakshmi and M. Prabu, Research Issues on Elliptic Curve Cryptography and its applications, IJCSNS VOL.9 No.6, June 2009.

[8]. K.M Akhil, P. Kumar,B.R Pushpa, "Enhanced Cloud Data Security using AES Algorithm",International Conference on Intelligent Computing and Control (I2C2), 2017.

[9]. "K. Archana , V. Sikri , "Comparative Analysis of RSA and ECC ", IJIRCCE 2015, p 49-52.

[10].R. Sinha, H. K Srivastava, S. Gupta, " Performance Based Comparison study of Rsa And Elliptic Curve Cryptography", International Journal of Scientific & Engineering Research, Volume 4, 2013,p 720-725.

[11].P. Yellamma, C. Narasimham, and V. Sreeniva, "Data Security in Cloud using RSA"," IEEE 2013.

[12].O. D Alowolodu, B. K Alese, A. O Alowolodu, O. S Adewale, "Elliptic Curve Cryptography for Securing Cloud Computing Applications", International Journal of Computer Applications Volume 66,2013, p 10-17.