Secure Data Transformation in Cloud Using Hybrid Cryptography

EBT Hansika[1#], RGC Upeksha[1] and T Weerawardane[2]

[1]*Department of Computer Science, General Sir John Kotelawala Defence University, Sri Lanka*
[2] *Department of Computer Engineering, General Sir John Kotelawala Defence University, Sri Lanka*

[#]36-cs-0007@kdu.ac.lk

Abstract*: The cloud is a very well-known and accepted data storage that provides many benefits to users with a pay-as-you-go pricing model, even providing storage solutions for massive amounts of data. Many users nowadays use different cloud services, mainly because the data can be accessed from anywhere via the internet. The cloud servers are located all over the world storing massive amounts of data. When a user uploads or downloads from the cloud server, the data is exposed to the internet. This can lead to security issues such as unauthorized disclosure of data and the privacy of users if the data is not properly protected. Many cryptographic algorithms are used to secure data transformation in the cloud. The proposed system is designed to offer a method for properly securing data when transferring them to the cloud, utilizing various cryptographic techniques, and integrating them most innovatively and effectively considering the security, data integrity, speed, and data confidentiality. The data is encrypted using a combination of three algorithms namely AES, ECC, and RSA by increasing the security of the data. The keys generated by the ECC and RSA are combined using an Exclusive OR gate. The AES key is uploaded into the key management server after being encrypted by the newly generated key. The data encrypted by the AES key are uploaded into the cloud storage. The proposed system is intended to distinguish the features and functionalities to overcome the drawbacks of the current systems.*

Keywords: *RSA, ECC (Elliptic Curve Cryptography), AES, Cloud, Key Management Server*

1. Introduction

Cloud computing is described as the delivery of computing services over the internet. The difference in cloud computing is, that the PC is in a cloud provider's data center instead of physically, and it provides services such as data storage, security, networking, software applications, and business intelligence via the internet. In Cloud Computing, a cloud vendor is responsible for the hardware purchase and maintenance. Unlike traditional storage systems, you can access your data and information stored in the cloud at anytime from anywhere on any device. Hence, the data stored on the cloud has the following threats when storing and retrieving data.

A. Data breaches can occur while revealing sensitive customer information, intellectual property, and trade secrets. Expose one's sensitive data by listening to the activity of a user on one virtual machine signaling the arrival of an encryption key on another VM on the same host.
B. The data stored at different locations increase the risk of unauthorized physical access to the data.
C. Sharing the data storage with multiple users increases access to your private information.
D. Denial of Service attacks and Distributed Denial of Service attacks.

E. The data is exposed to the internet when traveling over several networks leading to security issues such as unauthorized disclosure of data and privacy of users.

With the evolution of networking, both Asymmetric and Symmetric algorithms has the ability to secure the data transformation of the cloud using various techniques. ECC and RSA are two Asymmetric cryptographic algorithms that are most widely accepted and used to secure the data transformation in the cloud. AES is a Symmetric cryptographic algorithm that is used to encrypt a large volume of data easily.

Securing the data transformation in the cloud is helpful to protect one's data and save time as the data is one of the most important things for people as the damages and threats that can happen to the data in the cloud are dangerous

2. Background

A. Cryptography

The invention and study of protocols that prevent the public or third parties from accessing private messages are known as cryptography. Various aspects of information security, such as data confidentiality, data integrity, authentication, and non-denial, are central to modern cryptography. It can be described as a method of storing and transmitting data in a particular form so that only those who have the right can read and process it. Cryptography can be used for user authentication in addition to securing data against theft and modification. This protects sensitive information from disclosure while identifying the corruption and unauthorized change of information.

B. Symmetric Cryptography and Asymmetric Cryptography

Symmetric encryption is a form of data encryption that requires only one key(secret) for both encryption and decryption. Asymmetric encryption or public key encryption is a form of data encryption that requires two separate keys, private(secret) and public. These two keys are mathematically Connected. The public key is used to authenticate digital signatures or encrypt plain text, and the private key is used to decipher cipher text or create a digital signature.

C. RSA Cryptography

RSA was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978. The Rivest-Shamir-Adleman (RSA) is the most widely accepted and used public key cryptographic algorithm. This can be used for encryption and decryption, digital signatures, and for key exchanges. The plaintext and ciphertext of the block cipher RSA are both integers.

RSA algorithm involves three steps key generation, encryption, and decryption. Key generation is used to generate two keys the public key and the private key before the encryption takes place. The public key, accessible to anyone is used to encrypt the message and send it to a public channel. While the private key also known as the secret key is used to decrypt the message. The private key is only accessible by an authorized person *ECC (Elliptic Curve Cryptography)*

Elliptic curve cryptography (ECC) is one of the

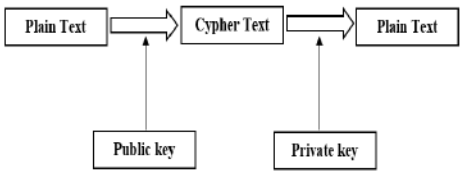


Figure. 1. RSA Cryptography

public key cryptographic schemes which uses

the characteristics of an elliptical curve to create Cryptographic calculations. ECC fully depends on the mathematical background. ECC requires far fewer and smaller parameters for encryption and decryption when compared to RSA. Other than traditional methods of generating keys as a product of very large prime numbers, the ECC uses properties of the elliptic curve equation. It is widely used for mobile applications as the ECC helps to achieve the same security with less computing power and battery resource usage.

Elliptic Curve

An elliptic curve is represented as a looping line that intersects two axes. This can be generated by using a binary
curve. The structure of the binary can be represented by the
following equation. (E, et al., 2019)

$$y^2 = x^3 + ax + b$$

'a' and 'b' are the constants that is used to define the curve while 'x' and 'y' are the standard variables that are used to define the function

The table 1 represents the key length of symmetric, RSA and ECC algorithms.

3. Realated Work

This section deals with the vast amount of research that depicts the evolution and development of cryptographic algorithms in different ways to secure data transformation in the cloud.

The researchers (Parsi & Sudha, 2012) have proposed a method to secure the data in the cloud by implementing the RSA algorithm. User data has been encrypted first and stored in the cloud, when the user places a request, the cloud provider authenticates the user and gives the data while providing the access to only authorized users. The user can decrypt the data with the corresponding private key. Even if an unauthorized person accesses the data, they are unable to decrypt the data and retrieve the original data.

The system proposed by (Ravi & Suresha, 2013) provides greater security services such as confidentiality in the cloud by using an ECC algorithm that contains advantages like smaller key sizes, less memory usage, and lower CPU time instead of using RSA for encryption. The researchers have used elliptic curve theory to create smaller, faster, and more efficient cryptographic keys and generate keys through the characteristics of the elliptic curve equation.

The research (S & A, 2017) has proposed a system to secure cloud storage using the ECC algorithm for encryption and decryption. The user is provided with a password, verification sign, and security level questions when he requests the cloud service provider to store a file in the cloud. The cloud service provider examines the data and encrypts and stores the data in the cloud server. When the user wants to access the data, the cloud service provider will decrypt the file and give it back to the user after the verification process. The researchers have depicted that the ECC algorithms for encryption are way better than when compared with the AES.

The research done by (Nikita , et al., 2016) has created a way to secure the cloud and data in cloud computing by using digital signatures and encryption with elliptic curve cryptography (ECC) as it provides a way better security as well as efficient performance than other public-key cryptographic techniques while providing the same level of security with less key size. Partitioning the private key and storing them in three different storage locations are the main objectives that have been focused in this paper to improve the security to authenticate the user's data, hence

it is difficult for the attacker to find the original private key.

The research done by (Varma, 2018) has explored the roles of ECC, RSA, and Diffie-Hellman algorithms in network security and in their applications in the industry through an analysis of its ubiquity in Secure Shell, Bitcoin along with the transport layer security. The study has depicted that ECC, RSA, and Diffie-Hellman algorithms provide benefits as well as disadvantages in network security.

The study (Manju , et al., 2016) has exposed data transference architecture for cloud computing using cryptography algorithms. The proposed system contains 3 basic steps, user identification and verification, secure data upload, and secure data transmission. The identification and verification process happens using the biometric technique. The second step is achieved using hashing and an efficient RSA technique. The data transmission happens with the help of the 3DES algorithm as the attacks that can occur with 3DES are less than compared with the DES algorithm. Even though the proposed system provides a highly secure environment, the researchers have described the hybrid encryption algorithm will be best in the near future to secure data transformation in the cloud as cloud computing will be the next IT revolution.

Another system proposed by (E, et al., 2019) has created three levels of key for the cryptography to avoid the GCD attack that can happen in RSA. The private key and public key of both RSA and ECC have been combined to generate a hybrid private and hybrid public key using an Exclusive OR to avoid the drawbacks of RSA algorithm such as GCD attack. Hence, the RSA encryption is done by using the new hybrid public key and RSA decryption is done by using the new hybrid private key providing a higher key strength than a simple key generation of the RSA algorithm. This research has exposed the fact that the combination of RSA-ECC gives the best results when compared to the RSA algorithm.

The research done by (XiaoChun , et al., n.d.) has proposed 3 cloud data storage models secure data backup, secure data sharing one to many and secure data sharing one to one by assuming that each user has two parts of data as private data and shared data; users' private and sensitive data is stored in the private data part while the data that can be shared with authenticated users are stored in the shared data part. The data is encrypted before uploading to the cloud using Symmetric cryptography algorithms while generating a key for each data separately. The integrity of the data is verified using the Hash of the data. Hence, these cloud data storage models provide cryptographic solutions to ensure that the users can share data and store data in the cloud with much security and efficiency. They have applied ECC to achieve low computation and communication costs with a less key size to provide the same level of security as RSA making the scheme more efficient.

The research (K, et al., 2021) has used a technique called double encryption to increase the security level of data in cloud storage. In this system, the file is encrypted twice using two algorithms, AES and RSA one after the other. When the user uploads a file, first the file is encrypted using AES generating the AES key and then by RSA algorithm generating the RSA key. A user needs to request the owner to download a file from the cloud. The owner has to send the corresponding key via email to the requested user. The researchers have stated the fact that this method provides high security with endurance against propagation errors while providing less runtime compared to other existing algorithms. Hence, the proposed

system is a secure and cost-effective method for the protection of data in cloud services.

The researchers (Nagasai & Supriya , 2018) have proposed methods to secure data in the cloud using AES, One Time Pad, and AES cryptographic algorithms. The study has exposed the Time and Space complexities of three hybrid models, RSA and AES, RSA and OTP, and RSA and OTP with variations, and has concluded that OTP with variation and RSA have lesser complexity (220ms) and are not easily attacked when compared with other hybrid models.

Another system proposed by (Z & MARRAKI, 2018) has created an architecture for inter-cloud data sharing to secure data stored in the cloud with encryption and decryption algorithms. The file which needs to be stored in the cloud is encrypted using the AES algorithm while the AES key is encrypted using the RSA algorithm and stored in the intern server. The user can download the data using the AES key after decrypting using the RSA algorithm.

Table 1. Comparison of Symmetric,

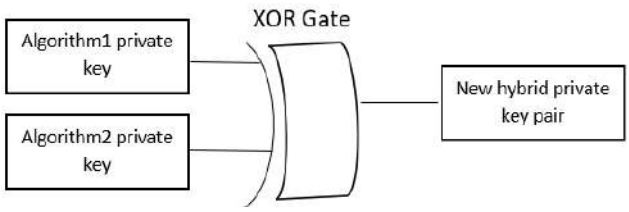
Symmetric Key Length	**RSA Key Length**	**ECC Key Length**
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

The research (Ming-quan & Peng-yu , 2016) has proposed ECC based homomorphic encryption method to reduce communication and computation costs for privacy protection of the cloud. They have concluded this method achieves better efficiency when compared with RSA and Paillier encryption algorithm.

4. Methadology

The main importance of this study is to provide an efficient method to secure the data when they are transferred to the cloud. The data is encrypted using a combination of three effective algorithms by increasing the security of the data. And, the generated key will be stored in another file and will be sent to the cloud Key Management Server. Even to reduce to risk of data disclosure if an attacker gains full access to the system, the key which is used to encrypt the data is being encrypted using a combination of another two algorithms. The two algorithms are combined using an Exclusive OR gate and generate a new hybrid key.

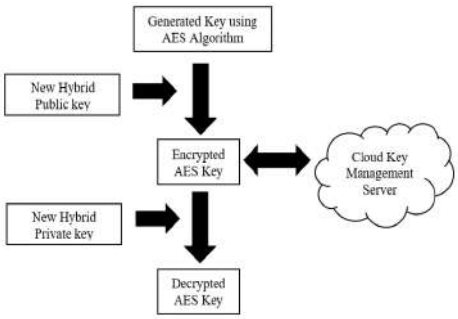
Fig 2. Combination of two algorithms using



XOR Gate

The system design is done by diving the whole system into two parts to secure the data and to secure the key.

A. Secure the key



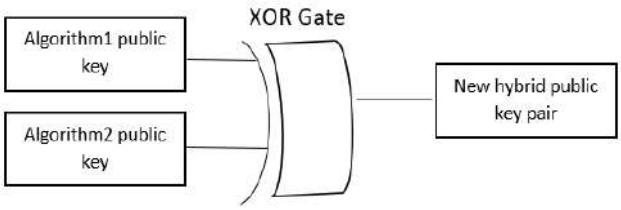


Fig 3. Secure the key

Combine two algorithms to generate a new hybrid public and hybrid private key. ECC and RSA algorithms are used to generate the new hybrid key. The private key of both ECC and RSA algorithms are used to generate the new hybrid private key and the public key of both RSA and ECC algorithms are used to generate the new hybrid public key. The hybrid keys are saved in the system, so unauthorized users cannot access the hybrid keys without correct credentials.

The hybrid public key is used to encrypt the AES key which is used the encrypt the data while the hybrid private key is used to decrypt the encrypted AES key. Then the encrypted AES key is uploaded into the Cloud Key Management Server. Even if an attacker gains access to the AES key, as it is being encrypted, unauthorized users cannot even decrypt the key in order to access the data.

B. Secure the data

First, the file is encrypted using the AES key and it is stored in the cloud with the encrypted AES key. When an authorized user accesses the file he cannot decrypt the file without the AES key. To do that, he wants to access the key management server or the place where the key is stored. As the AES key is encrypted with the hybrid key, even though an attacker received the AES key, he won't be able to decrypt the key and gains access to the data. So, the user data is fully protected through the system even if the attacker gains full access to the cloud storage.

5. Discussion

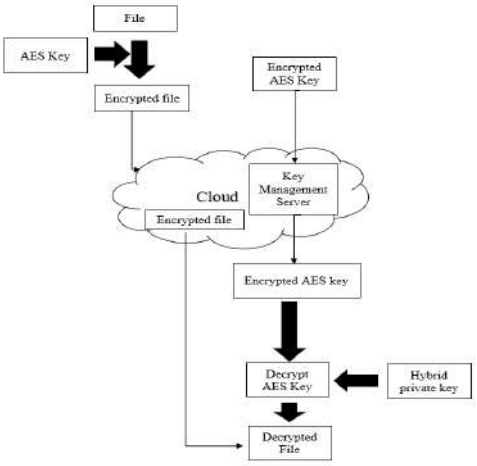


Fig 4. Secure the data

Data transformation in the cloud can be secured using various cryptographic algorithms with different techniques. According to the researches, the mainly used and effective techniques for secure data transformation in the cloud are as follows:

A. Use of ECC algorithm.
B. Use Double Encryption.
C. Use of RSA algorithm.
D. Hybrid key generation

Key generation time, execution time, and security of data are the main characteristics that are used to evaluate the performance of cryptographic algorithms.

A. Use of ECC and RSA algorithm

The table 1 shows the RSA and ECC comparable key sizes with corresponding Security levels.

The main advantage that nowadays most people are using the ECC algorithm is that less key size. According to table 1, it can be seen that a 160-bit key is equivalent to the 1024-bit key in RSA. (Ariffin & Mahad, 2012)

Table 1. Comparison of RSA and ECC

Parameters	ECC	RSA
Key generation	Faster	Slower
Execution time	Faster than RSA	Slower than ECC
Security	High	High

Table 2 shows that the key generation time is fast in ECC. In both ECC and RSA the key generation time is somewhat equal for smaller key sizes. But when the key size grows, RSA takes much amount while ECC remains almost the same. ECC provides faster execution time for smaller key sizes while RSA takes much time as it uses higher key sizes.

B. Use Double encryption

Double encryption is mainly used to increase the security of the system. Two algorithms are used one after the other. The data is encrypted first using one algorithm and then again by the second encryption algorithm.

Table 2. Time Complexities of Hybrid Models

Hybrid models	Time complexities (milliseconds)
RSA and AES	1020
RSA and OTP	533
RSA and OTP with functions	220

According to table 3, RSA and OTP with functions have less time complexity compared with the other two algorithms and it is much more efficient.

C. Hybrid key generation

ECC public key is exclusive OR with a RSA public key to generate a new hybrid public key and ECC private key is exclusive OR with a RSA private key to generate a new hybrid private key. The new hybrid public is used to encrypt the file while the new hybrid private key is used to decrypt the file. (E & Rathipriya, n.d.) Table 4 shows the execution time in milliseconds corresponding to the file size.

Table 3. Execution time of different file sizes in Hybrid key generation

File size	Execution time in milliseconds
10 KB	3.5
20 KB	2.7
25 KB	6.8
54 KB	9.8

D. Attacks

Attackers can use different types of attacks, depending on the different cryptographic algorithms.

Table 4. Different attacks according to different algorithms

Algorithm	Attacks
RSA	Timing Attacks (Guess the encryption key by tracking the time to perform its crypto operation)
AES	Side channel attacks (Try to physically attack the implementation of the cryptographic system)
OTP	Brute force attack (Use all possible keys to discover the correct key)
ECC	Side-channel attacks Twist-security attacks

6. Conclusion

On this basis, it can be concluded that much research has been done in recent decades with the aim of researching new technologies to secure data transformation in the cloud. Unlike

traditional storage systems, data that are stored in the cloud can have various threats when storing and retrieving data. To overcome these drawbacks, we have discussed four mainly used techniques and algorithms, ECC, RSA, Double encryption, and hybrid key generation along with their performance characteristics. After analysing these techniques and algorithms we can conclude that the use of these techniques also has some drawbacks. Hence, hybrid key generation of ECC and RSA algorithms are used to generate a new key and the AES key is encrypted using the newly generated hybrid key by increasing the security of the proposed system. AES algorithm is used to encrypt a large volume of data easily. The data encrypted with the AES key and the encrypted AES key is stored in the cloud storage and key management server respectively increasing the security and reducing the time complexities of the proposed system. Hybrid key generation increases the key strength as well as execution time when compared with other techniques and methods. It can be stated that the proposed system is much more efficient and secure.

Acknowledgment

This research was greatly supported by General Sir John Kotelawala Defence University and I would like to pay my gratitude to the lecturers of the Faculty of Computing for their guidance.

References

Ariffin, M. & Mahad, Z.(2012). Public Key Cryptosystem – A Comparative Analysis Against RSA and ECC. s.l., *7th International Conference on Computing and Convergence Technology (ICCCT)*.

E, V. R. & Rathipriya, n.d. Comparative Study of Hybrid RSA-ECC and Hybrid DNA-Insertion for Large Dataset. *International Journal of Grid and Distributed Computing.*

E, V., S, S. & R, R., 2019. *HYBRID KEY GENERATION FOR RSA AND ECC.* s.l., Fourth International Conference on Communication and Electronics Systems.

K, J., Shirley, S., Sahana, S. & Thanmai, G. (2021). Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm. Pune, *International Conference on Emerging Smart Computing and Informatics (ESCI)*.

Manju , K., Manoj , K. & Vaishali. (2016). Secure Data Transference Architecture for Cloud Computing using Cryptography Algorithms. *International Conference on Computing for Sustainable Global Development.*

Ming-quan , H. & Peng-yu , W. (2016). Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing. *IEEE International Conference on Intelligent Data and Security*.

Nagasai, L. K. & Supriya , M. (2018) . Secure Data Storage in Cloud using Cryptographic Algorithms. *Fourth International Conference on Computing Communication Control and Automation.*

Nikita , N. C. et al. (2016). *Enhancing Cloud Data Security Using Elliptical Curve Cryptography*

Parsi, . K. & Sudha, . S. (2012). Data Security in Cloud Computing using RSA Algorith. *International Journal of Research in Computer and Communication technology,* 1(4).

Ravi , G. & Suresha. (2013). Enhancing Security in Cloud Storage using ECC Algorithm. *International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064,* 2(7).

S, S. & A, A. (2017). Effective Secure Data Storage in Cloud by Using ECC Algorithm. *Middle-East Journal of Scientific Research.*

Varma, C., (2018). IEEE International Conference on Current Trends toward Converging Technologies, Coimbatore, India.

XiaoChun , Y., ZengGuang, . L., Young, L. S. & Hoon , L. J., n.d. *PKI-Based Cryptography for Secure Cloud Data Storage Using ECC.* s.l., s.n.

Z, K. & MARRAKI, M. E. (2018). *Using Encryption Algorithm to enhance the Data Security in Cloud storage.* s.l., ResearchGate.

Authors Biography

EBT Hansika is a final year undergraduate of General Sir John Kotelawala Defence University. Following the BSc (Hons) Computer Science Degree Programme. Studied at Ferguson High School, Rathnapura

RGC Upeksha obtained her BSc (Hons) in Software Engineering degree from General Sir John Kotelawala Defence University. The main research interests include Cybersecurity, Computer and network security and Cryptography.

Prof. Thushara Lanka Weerawardane was graduated in Electrical Engineering from the University of Moratuwa in 1998 and consequently he received MSc Degree "Communication and Information Technology" in 2004 and received Ph.D. from the University of Bremen, Germany in 2010. Prof. Thushara Lanka Weerawardane worked in Kotelawala Defence University as senior lecturer Gr.1 from 2012 to 2016 during this period he held several academic and administrative positions such as Head of the Department and Dean, Faculty of Engineering. Currently, he is working in Kotelawala Defence University as Professor.