ISSN: 2229-6956 (ONLINE)
DOI: 10.21917/ijsc.2019.0268

HYBRID CRYPTO SYSTEM USING HOMOMORPHIC ENCRYPTION AND ELLIPTIC CURVE CRYPTOGRAPHY

R. Hemanth Kumar, T. Arvind, V. Bharath Narayanan and Prabakeran Saravanan

Department of Computer Science and Engineering, K.C.G college of Technology, India

Abstract

Providing security and privacy for the cloud data is one of the most difficult task in recent days. The privacy of the sensitive information ought to be protecting from the unauthorized access for enhancing its security. Security is provided using traditional encryption and decryption process. One of the drawbacks of the traditional algorithm is that it has increased computational complexity, time consumption, and reduced security. We proposed a scheme in this the original data get encrypted into two different values. Using Elliptical curve cryptography (ECC) and Homomorphic are combined to provide encryption. The data in each slice can be encrypted by using different cryptographic algorithms and encryption key before storing them in the Cloud. The objective of this technique is to store data in a proper secure and safe manner in order to avoid intrusions and data attacks meanwhile it will reduce the cost and time to store the encrypted data in the Cloud Storage

Keywords:

Security, Privacy Preservation, Homomorphic Encryption and Decryption, Key Generation

1. INTRODUCTION

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server. Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. Applications that keep running in the cloud can balance various components including load balancing, bandwidth, security and size of data. A major issues to cloud adoption is data privacy and security, because the data proprietor and the service supplier are not inside the similar confided in domain. Safety issues are increasingly significant in most reduced layer infrastructure as a Service (IaaS) to higher platform as a Service (PaaS).

The data has a few stages throughout its life time. These stages are - create, transfer, use, share, storage, archive and destroy. The information needs security at all these stages. An information security lifecycle alludes to the whole procedure from information creation to its expulsion from cloud.

This paper centers on security of cloud data very still. Confidentiality to the data can be given by utilizing encryption. At the point when data is encrypted it isn't actually comprehended by unauthorized individuals and to get plain content back decryption process is utilized. For performing calculation there is a need to decrypt the data first. Encryption fathoms serious issues. The intensity of distributed computing can be used, if client or application can complete calculation on encrypted data.

Homomorphic encryption procedure is a type of encryption that enables explicit kinds of computations to be performed on encrypted data and creates an encrypted outcome. The decrypted aftereffect of any task is indistinguishable such from working straightforwardly on plaintexts [1]. The capacity to perform computations on cipher texts without knowing any data about the plaintexts makes this system valuable in a wide assortment classification saving conventions. The major contribution of the research is given below.

- First the original data is encrypt using Elliptic curve cryptography to provide data security.
- Second encrypt the data is given to another cryptographic algorithm and the output is stored in cloud.
- Decryption is done using both Elliptic curve algorithm and homomorphic algorithm

The following sections of this paper are ordered below: the existing encryption and key generation mechanisms for cloud data privacy preservation are surveyed with its advantages and disadvantages in section 2. The proposed methodology is explained in detail with its step by step illustration in section 3. The performance analysis of the both existing and proposed mechanisms are evaluated in section 4. The conclusion and future work of the paper are stated in section 5.

2. RELATED WORKS

In this section, we are going to see about works related to data security, different types of encryption and decryption techniques.

In [2] different ways of securing data privacy and confidentiality using homomorphic encryption for storing data in the cloud. Homomorphic encryption is encryption standard that allows the user to do calculations on the encrypted data and decrypted result also shows the same results as the original data. Homomorphic encryption is of two types they are Partial Homomorphic encryption (PHE) and Fully Homomorphic encryption (FHE) while in PHE we can only do multiplicative operation but fully homomorphic can do both additive and multiplicative operations.

In [3] developed a Hybrid Data Encryption Technique for securing cloud data. Here Blowfish and RSA used for encryption and decryption and digital signature used for authentication. It’s implemented using Xilinx ISE 14.1. It can be implemented for both symmetric and asymmetric algorithms. Its cost efficient because blowfish is open source algorithm.

In [4] investigates weather Homomorphic encryption can be implemented or not in hybrid system. Homomorphic encryption are used in variety of field in e-voting Hospitals, etc. Since fully homomorphic encryption still under experimentation we can over this defect by introducing to hybrid crypto system with homomorphic encryption what are the ways to do that.

In [5] developed a new hybrid encryption standard using homomorphic encryption. In this paper they used Paillier algorithm which is used additive operation in homomorphic and RSA encryption is used for Multiplicative operations in Homomorphic. Here encryption process run on the private cloud and cipher text is stored in the public cloud.

In [6] developed homomorphic encryption for network coding. Homomorphic signatures that can be utilized to secure the integrity of network coding. He proposed a RSA based homomorphic signature plot as of late for this reason. We demonstrate that their plan in reality does not fulfill the required homomorphic property, and further, despite the fact that it very well may be settled effectively, still no message forgery attacks.

In [7] developed an Attribute based encryption on hybrid cloud system. Here he developed a most centralized frameworks permit information access to its cloud user if a cloud user has a certain arrangement of satisfying attributes. One technique to contend such policies is to utilize an authorized cloud server to maintain the user information and have get to command over it. When one of the servers keeping information is compromised, the security of the user information is compromised. For getting access control, maintaining information security and obtaining precise computing results, the information proprietors need to keep attribute-based security to encode the put away information. During the delegation of information on cloud, the cloud servers might be altered by the counterfeit cipher-text. Besides, the authorized users might be bamboozled by retorting them that they are unauthorized. Generally the encryption control get to attribute policies are unpredictable. In this paper, we present Cipher-text Policy Attribute-Based Encryption for maintaining complex access command over scrambled information with verifiable customizable authorization. The proposed technique provides information confidentiality to the encoded information regardless of whether the capacity server is comprised. Besides, our strategy is highly verified against collusion assaults. Ahead of time, execution evaluation of the proposed framework is explained with implementation of the equivalent.

In [8] developed a modified Elliptic curve algorithm for enhanced cloud security. The data is encoded and decoded by using the similar MECC calculation. Here the clients and other administrators need to get to the cloud data, they are confirmed using authentication. After the authentication, the requesters are given with traits. The collectors execute the MECC calculation and create private key for decoding the data with these properties. This guarantees high level of data epitome in cloud calculation. Execution correlation between the proposed and traditional plans are done and saw that the MECC calculation is very secure than other customary plans.

In [9] developed an ElGamal Elliptic Curve Cryptosystem for Cloud Server Aided Computation. The cloud server aided cryptosystems are utilized to assist clients with finishing complex encryption/decoding computation, and client's wont stress over information spillage. Here author suggest another cloud server aided computation for ElGamal Elliptic Curve cryptosystem. Notwithstanding giving related cloud administrations clients, the proposed conventions can keep some dynamic attacks also, passive attack.

Anjali Baburao Jivane.[10] developed a Time Efficient Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data. Here among different multi-watchword semantics, we pick the productive likeness proportion of arrange coordinating, i.e., however many matches as could be expected under the circumstances to catch the pertinence of data archives to the search question. We further utilize internal item closeness to quantitatively assess such likeness measure. Author propose an essential thought for the MRSE dependent on secure internal item calculation to proficiently accomplish multi-keyword ranked search and afterward give two fundamentally enhanced MRSE plans to accomplish different protection.

In [11] developed an Authenticated CRF based Improved Ranked Multi-keyword Search for Multi-owner Model in Cloud Computing. Here the privacy preserving ranked multi keyword search framework for multiple information owners (PRMSM). This framework permits the protected search with device entryway by utilizing secure search convention and moves forward the search effectiveness by utilizing Conditional Random Field (CRF) strategy. This strategy is a mix of tokenization, POS labeling and score computation. It is utilized to expel the undesirable information alongside diminishing the list estimate which prompts progressed search effectiveness. The exploratory outcomes demonstrates that the framework keeps up the security, privacy, realness alongside moved forward search effectiveness and positioning of results to enhance the experience of searching. This framework likewise underpins the component of client renouncement.

In [12] developed a data storage using Advanced Encryption Standard algorithm and Proxy Re-encryption. Here when the storage framework is scattered and has no focal power. Here, a proxy re-encryption conspire is recommended and joined with a distributed erasure code with the end goal that a secure and solid information storage and retrieval, however likewise lets a client to share his data on the cloud with a different client in the encoded arrangement itself. This paper encourages the utilization of encoding the scrambled documents and sharing records in the encoded position itself. This paper utilizes the systems of both encoding and sharing the information. Erasure encoding bolsters sharing encoded documents and is substantial in decentralized distributed framework. A distributed erasure code is utilized to approve the information security in the scattered cloud storage.

3. PROPOSED WORK

In Section we see how the data in the cloud can be stored securely. The fundamental process is to build up a secure framework for securing the privacy of the cloud information. Here, a homomorphic– elliptic curve Cryptography is developed for securing cloud data storage. The environment where both the public and private qualities are integrated is Multi-cloud. Homomorphic encryption permits the utilization of mathematical operation on encrypted data so the decrypted data would have same applying matching operations on unencrypted data. Encryption is the process of encoding information in such a way that hackers cannot read it. There are two types of encryption techniques. ECC and Homomorphic. The data in each slice can be encrypted by using different cryptographic algorithms and encryption key before storing them in the Cloud. The goal of this system is to store information in a legitimate secure and safe way so as to stay away from intrusions and data attack mean while it will diminish the expense and time to store the encrypted information in the Cloud Storage. Elliptic curve cryptography is used to store the data in an encrypted form while the homomorphic algorithm is symmetric key cryptography. The Fig.1 shows the architecture diagram of the proposed system.

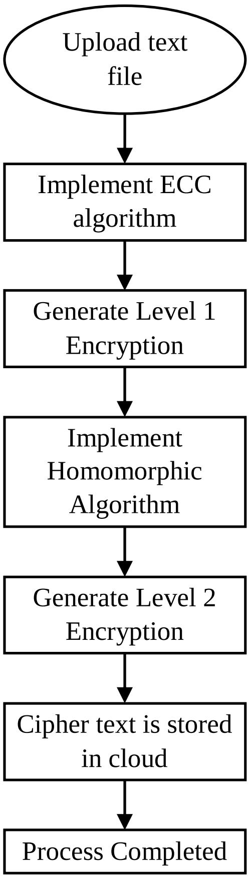
Upload text file
Implement ECC algorithm
Generate Level 1 Encryption
Implement Homomorphic Algorithm
Generate Level 2 Encryption
Cipher text is stored in cloud
Process Completed

Fig.1. Architectural of the Proposed System

Some of the stage of the proposed system are given below.

- Key Generation
- Encryption
- Decryption

First using the key generation algorithm both the public and private keys are generated and the data are encrypted using the keys first using the Elliptic curve algorithm and then cipher text is again encrypted using the homomorphic algorithm and then stored into the cloud. For the decryption process the encrypted data is forward to the user and their decryption algorithm is applied to encrypted data to decrypt the cipher text and get the original text.

3.1 KEY GENERATION

Elliptic Curve Cryptography is a public key cryptography algorithm. It was first designed for digital signature purpose only but later modified into encryption and decryption purpose also. The strength of algorithm is based on discrete logarithm.

Step 1: Choose a random prime number a.

Step 2: Choose a two random number b and c where $(b<a)$ and $(c<a)$.

Step 3: Calculate $d = b^c$ mod a.

Step 4: D is the public key and c is the private key and a and b are both public.

Prime number a which is selected at random is a public. Then another two random number are selected where one is public and private in this b is public whereas c is private. Key generation can be of various size security will as the key increases and computational time is also increased as the key increased. This is one of the disadvantage of the key generation.

3.2 ENCRYPTION

Encryption is the process in which plaintext or the data is encoded in such a way that even though the file can be seen it can identified because it is encoded. Encryption is technique which is used in data security till today. Elliptic curve cryptography is a new age encryption technique where encryption is public while the decryption is made in private. It provide security by all the algorithm thus it provide security in cheap cost when compared other algorithm. It also provide the secure transmission of key between the end user.

Input: Public key and data file.

Output: Encrypted data.

Step 1: Generate the public key.

Step 2: $K_{pu} = k_{pr} * g$ where g is the generating function.

Step 3: Cipher is generated $c_p = r * g$.

Step 4: Data file is encrypted using $d = r * k_{pu} + (i_n * p_c)$.

Step 5: Again encrypt using the homomorphic function.

Step 6: Data is stored

If the Paillier public key is (N,g), private key is (p_r,p_u) then for the plain text m choose a random number r_s. The Encryption process is

$$C = g^m * r_s \bmod n*n$$

It is most suitable for the data security and privacy problem in the cloud. Elliptic curve cryptography and homomorphic are used to store data in cloud securely. In this algorithm the private key and the input data are given as the input. And then using generating function g in curve public key is created k_{pu}. Similarly cipher text is generated by using four random number r_s. And then the input data is encrypted using the random function on cipher text with the public key we generated. The output is the encrypted data which is stored in the file.

3.3 DECRYPTION

Decryption is process in which encrypted text or the data decoded and then we can see the original file. Once the user request for data file the homomorphic process is applied to the encrypted data. And then the Elliptic curve cryptography is applied to the cipher text which is produce by the homomorphic process and the private key is used to decrypt the whole process and after this process is we can get the original data.

Private Key and the encrypted data is taken as the input for this process and output produced will the original file which is encrypted. First step we take the private key and the encrypted data we produce the cipher text. Next we take the random number we have taken with private key and generated function g from the curve. For the decryption the process again repeated with the public key and the output is subtracted from the private key cipher text and the original output is produced. One the key challenges of the process is that key size produced by different algorithm is found to different and the algorithm is executed in such that it should be equal.

We should provide authentication to cloud provider so that there will intruder in the cloud environment. There are many method to this such as authentication and authorization process and many protocol are used now a days to security to the cloud so the correct user can only we accessing the cloud platform.

Input: Private Key and the encrypted data.

Output: Original data.

Step 1: Private Key for decrypting data.

Step 2: Cipher is extract from encrypted and the private key $c = d * kpr$

Step 3: Random value from generating function.

Step 4: Calculate $C_p = k_{pr} * (r_s * g)$

Step 5: Original data = $c + d - C_p$.

Step 6: Original data is extracted.

4. PERFORMANCE ANALYSIS

This part deals with the comparison of both proposed system and the traditional algorithm under certain parameter such as execution time, decryption and encryption timing. Following existing work can be used for comparison such as enhanced MORE algorithm and PORE algorithm which is used for the comparison.

4.1 EXECUTION TIME

Execution time is said to be time required for the cloud storage to access the data. The Fig.2 shows the comparison between execution time of the different algorithm. It is also included the time required by the cloud storage server to store the data in the encrypted form and also the time required to access it. The *x*-axis contains the keys sizes with the *y*-axis contains the time in milliseconds.

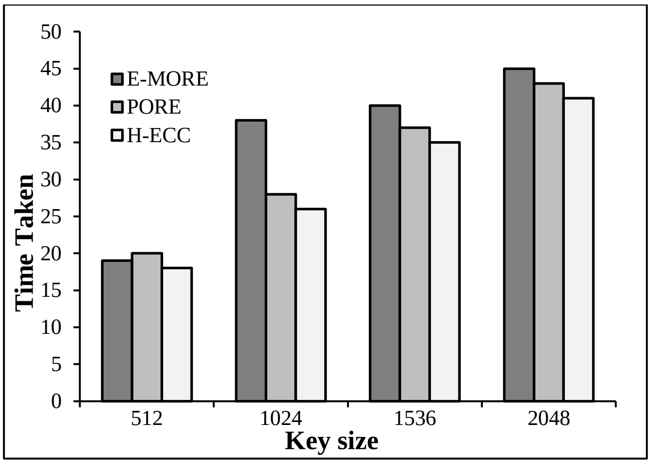

Fig.2. Execution time comparison of proposed and existing system

4.2 ENCRYPTION TIME

Encryption time is the timing requires to encrypt the data. It also can be expressed as the ending timing-starting timing. The Fig.3 shows the encryption timing comparison of the various algorithm and the proposed system. We analyze the result using various parameter such as keys size used for encryption and the time to execute the system. Form this analysis we can say that the proposed system is more efficient when compared to the existing ones.

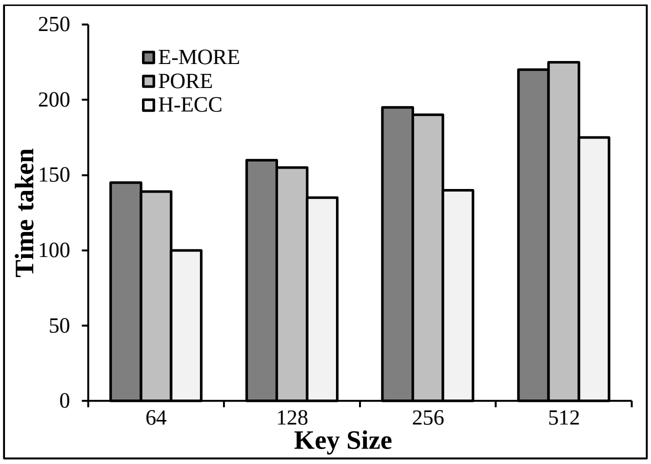

Fig.3. Encryption Time Comparison

4.3 DECRYPTION TIME

Decryption time is the amount of time requires for the particular algorithm to decrypt the encrypted data. Time increases as the key size increases. It can also be denoted as the ending time-starting time. Here we analyses it with the various algorithm in with various parameter such as key sizes and the time taken to execute. The Fig.4 we can see that our proposed system decryption timing is less when compared to existing algorithm.

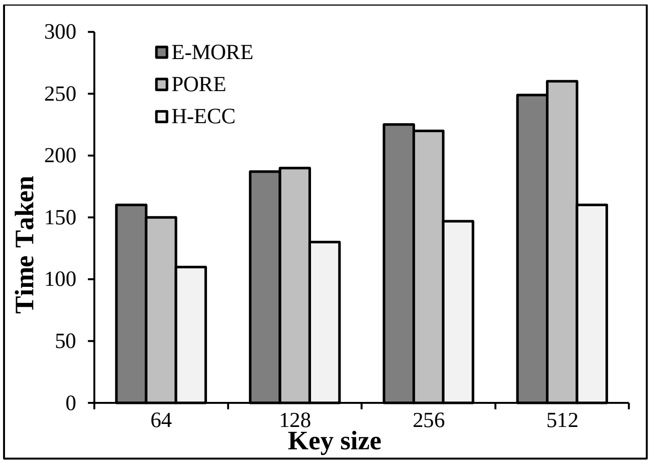

Fig.4. Decryption Time Comparison.

5. CONCLUSION AND FUTURE WORK

To overcome the limitations and disadvantage of the existing work we introduced a new framework which ensures the security and privacy of the cloud environment for data storage. This framework consists of three main modules they are key generation, encryption and decryption. First the data is encrypted using elliptic curve cryptography and homomorphic encryption. User can request the cloud provider and the cloud provide checks weather the user is who he told to be using any identity check protocol or mechanism. Many cloud provider uses access control polices to check the user identity and then encrypt that data using the above explained algorithm and the encrypted data is stored into cloud. Decryption process is same as the encryption one. In this private key is used as the main and encrypted data is decoded using the decryption algorithm. There are many ongoing research in field of cloud security and privacy some of the research work are Homomorphic encryption is used to provide outsourcing the calculations in the cloud which is used in case of data auditing. Since fully homomorphic encryption is newly introduced and its better than partial homomorphic encryption it is used in many hybrid cloud encryption process to calculated on the encrypted data. Fully homomorphic process can be used in search engine for privacy preservation. It is one of main ongoing research in many company. As of now, we are going to implement this as a prototype model only so there is nothing regarding with the cost factors involved here. When it is going to be implemented in terms of hardware level then we have to go and think about the cost factors.

REFERENCES

[1] V.P. Bansal and S. Singh, "A Hybrid Data Encryption Technique using RSA and Blowfish for Cloud Computing on FPGAs", *Proceedings of 2nd International Conference on Recent Advances in Engineering and Computational Sciences*, pp. 103-108, 2015.

[2] K. El Makkaoui, A. Beni-Hssane and A. Ezzati, "Can Hybrid Homomorphic Encryption Schemes be Practical?", *Proceedings of 5th International Conference on Multimedia Computing and Systems*, pp. 1-7, 2016.

[3] Y.S. Gunjal, M.S. Gunjal and A.R. Tambe, "Hybrid Attribute Based Encryption and Customizable Authorization in Cloud Computing", *Proceedings of International Conference On Advances in Communication and Computing Technology*, pp. 1-5, 2018.

[4] K. Raja and S. Pushpa, "Novelty-Driven Recommendation by using Integrated Matrix Factorization and Temporal-Aware Clustering Optimization", *International Journal of Communication Systems*, pp. 1-16, 2018.

[5] N. Lee, Z. Chen and F. Chen, "Cloud Server Aided Computation for ElGamal Elliptic Curve Cryptosystem", *Proceedings of IEEE 37th Annual Computer Software and Applications Conference Workshops*, pp. 22-26, 2013.

[6] R. Nivedhaa and J. Justus, "A Secure Erasure Cloud Storage System using Advanced Encryption Standard Algorithm and Proxy Re-Encryption", *Proceedings of International Conference on Communication and Signal Processing*, pp. 1-6, 2018.

[7] X. Song and Y. Wang, "Homomorphic Cloud Computing Scheme based on Hybrid Homomorphic Encryption", *Proceedings of International Conference on Computer and Communications*, pp. 13-16, 2017.

[8] A. Sude and V. Shinde, "Authenticated CRF Based Improved Ranked Multi-Keyword Search for Multi-Owner Model in Cloud Computing", *Proceedings of International Conference on Computing, Communication, Control and Automation*, pp. 1-5, 2017.

[9] M. Thangapandiyan, P.M. Anand and K.S. Sankaran, "Enhanced Cloud Security Implementation Using Modified ECC Algorithm", *Proceedings of International Conference on Communication and Signal Processing*, pp. 12-17, 2018.

[10] D.R. Kumar Raja and S. Pushpa, "Diversifying Personalized Mobile Multimedia Application Recommendations through the Latent Dirichlet Allocation and Clustering Optimization", *Multimedia Tools and Applications*, pp. 1-20, 2019.

[11] A. Yun, J.H. Cheon and Y. Kim, "On Homomorphic Signatures for Network Coding", *IEEE Transactions on Computers*, Vol. 59, No. 9, pp. 1295-1296, 2010.