International Research Journal of Education and Technology
ISSN 2581-7795

Integrated Cryptographic Algorithms to Enhance the Security on the Client Data Sharing System

Karthick M[1], Gokul S[2], Gokula Krishnan D[3], Jeevaananthan B S[4], Logeshwaran B[5]

[1]Assistant Professor, [2,3,4,5]UG Students - Final Year, Department of Computer Science and Engineering, Nandha College of Technology, Perundurai – 638052, Tamilnadu, India

Abstract

Now a day's individuals store their information on distributed cloud storage. Security is a significant issue in putting away information on cloud environment. Cryptography methods are extremely valuable to force security on information. A mixture cryptography framework is proposed to give better security on the information which is put away on distributed storage.The proposed approach utilizes RSA, AES, DH and ECC give a cross breed of the fouralgorithms to give greater security on the information prior to putting away it on cloud.The venture will be exceptionally helpful for IoT applications putting away information on cloud. The algorithms are compared with each other using three parameterssuch as Encryption length, Execution time and Memory usage and it is executed in JAVA and tested on aplain text. It is confirmed that the proposed algorithm is functioning admirably to give greater security on information.

Keywords: Cloud computing, RSA, AES, DH, ECC, cryptography, data security.

1. Introduction

The expression "Cloud computing" is a new popular expression in the IT culture. Behind this extravagant idyllic expression there lies a genuine image of things to come of figuring from both in specialized point of view and social viewpoint. Cloud computing is pointed toward giving IT as a support of the cloud clients on-request premise with more noteworthy adaptability, accessibility, dependability, and versatility with utility registering model. Data storage and security are the important factors in cloud computing [2],[9]. The proposed project deals with data security [6]. It uses four algorithms and gives a crossbreed calculation to improve the security [2],[3]. The introduction of cloud computing is extremely late peculiarities despite the fact that its root has a place with a few old thoughts with new business, specialized and social viewpoints. According to the structural perspective, the cloud normally expands on current network-based engineering and uses the framework administrations, and adds a few innovations like virtualization and some plans of action [7].

2. Related Works

In the Existing system, a Data Sharing system model, multiple user security that may encrypt in their own ways, possibly using different sets of cryptographic keys [2]. Every user obtains keys from every owner who's their central idea talks about the impossibility of Fully Homomorphic Encryption (FHE) alone for VM Cloud privacy [1],[3]. That classification hierarchy of VM Cloud Computing is not a standard model and has a few defects as we would discuss duly [5]. The system states the security and privacy issues from standard VM Cloud Computing definitions and discusses the challenges involved not just for FHE but also for many other techniques, but this requires too much trust in a single authority [5].Elliptical Curve Cryptography is an arrangement in which the keys needed to decrypt encrypted data are held in ECC so that, under certain circumstances, an authorized third party may gain access to those keys [2]. These third parties may include business, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications. It requires more resources for rekeying because it is being done for individual join/leave operation. It occupies high Memory usage and encryption key length [4]. The data transmission time and execution time is high.

NunoSantosh, Krishna P. Gummadi and Rodrigo Rodrigues propose Cloud figuring foundations authorize organization to lower expenses by reexplore computation on-request. However, clients of distributed computing administration at present have no method for checking the privacy and genuinely of their information and computation [4].To resolve this issue to propose the plan of a believed distributed computing stage (TCCP) [4]. TCCP empowers Infrastructure as a Service (IaaS) suppliers, for example, Amazon EC2 to give a shut box implementation climate that ensures classified implementation of visitor virtual machines [8].

Joshua Schiffman and his co-creators proposes the paper for the client's security basic information handling needs are starting to push back unequivocally against utilizing distributed computing [2]. Cloud sellers run their calculations upon cloud gave VM systems, but clients are concerned such host frameworks will most likely be unable to safeguard themselves from assault, guarantee disconnection of client handling, or burden client handling accurately[1],[7]. To give confirmation of information handling security in cloud to clients, client advocate techniques to further develop cloud straightforwardness utilizing equipment-based verification systems.

3. Proposed System

In the proposed system, wedeal with the problems present in the existing system. The Existing system has high Execution time, Memory usage and Encryption length. The proposed system helps to minimize those parameters. To implement the proposed system, we use four cryptographic algorithms.

Here it is the endeavor to study the patient centric, solves the problem of evaluating a function jointly by multiple parties on their private inputs secure sharing of file sharing in VM Cloud stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. It also no assumptions are made on computational resources available with the parties. All the parties would carry out same amount of work which is contrary to VM Cloud Computing setting. To adapt these techniques for an asymmetric setting like VM Cloud Computing where the server has massive amounts of computing power relative to the users, in order to protect the personal health data stored on a semi-trusted server, we adopt **Diffie Hellman** is better than **ECC** as the main encryption primitive. In proposed system a client is sharing some data with the other clients,here the data is in text format by using the combination of four algorithms, and the encryption process was executed. After the successful encryption a key will generate randomly then the client is sharing a file with another client. By using the generated key, the receiver decrypts the file and views the information in the file.

The proof techniques for making assertions about the complexity of one problem on the basis of another is called reduction “Using DH, access policies are demonstrate based on the attributes of users or data, which enables a patient to judicious share her file sharing among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. The complexity per encryption, key generation and decryption are only linear with the number of attributes involved. In proposed system, resources used for rekeying is reduced because it is being done for batch of join/leave operations. More secure by Boolean logic minimization because session management done by this concept.

3.1 Registration and Encryption

The client module the client program was carried out utilizing Java servlets and a JFrame page that conjures the servlet. The client enters the information to be sent through the JFrame page which then summons the Client servlet. The servlet then encodes this information utilizing the common key article created by the Diffie-Hellman Key Agreement calculation and the Data Encryption Standard (in ENCRYPT mode) and send it over to the server. The client served utilizes URL Redirection to send the scrambled message from the client to the server.

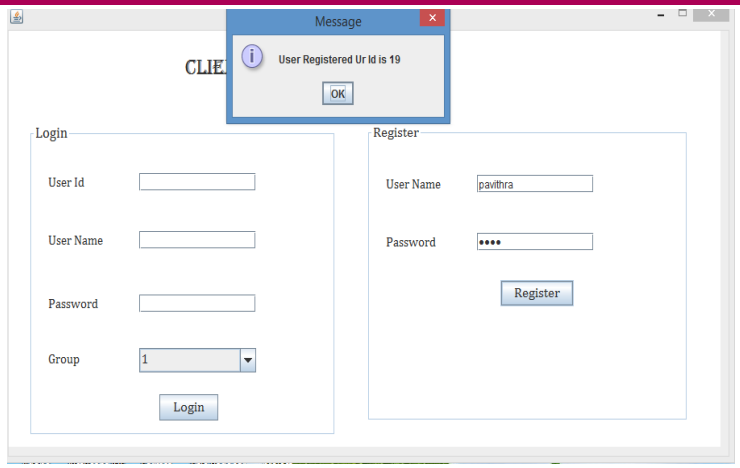

Figure 1Registration

Figure 2Login

Figure 3File encryption

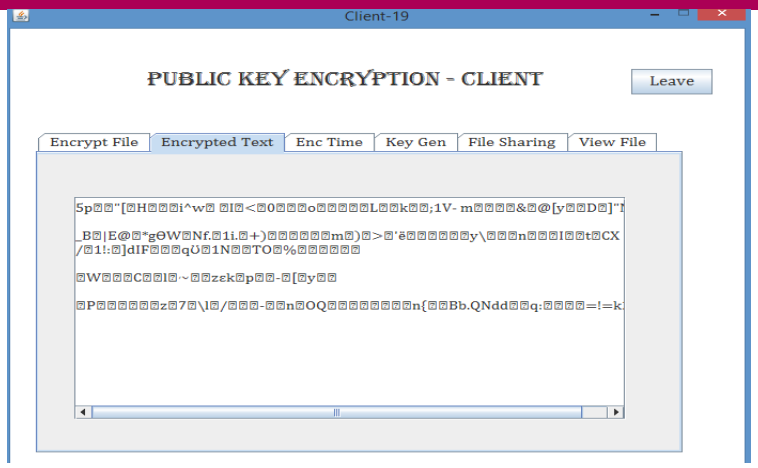

Figure 4Encrypted file

3.2 Database Storage

The actual server is a basic servlet that is associated with a data set. It gets the scrambled message from the client and unscrambles it utilizing the common key item created by the Diffie-Hellman calculation and Diffie Hellman (in DECRYPT mode).When the message has been encrypted the server will store the message into the information base, which can be recovered at a later stage.

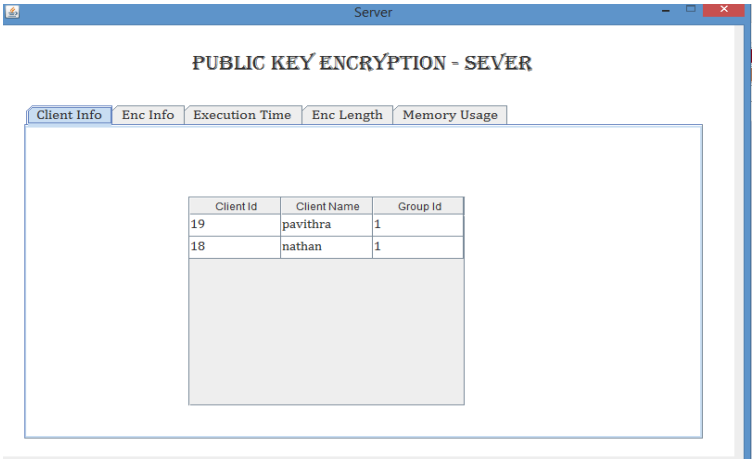

Figure 5Client Information

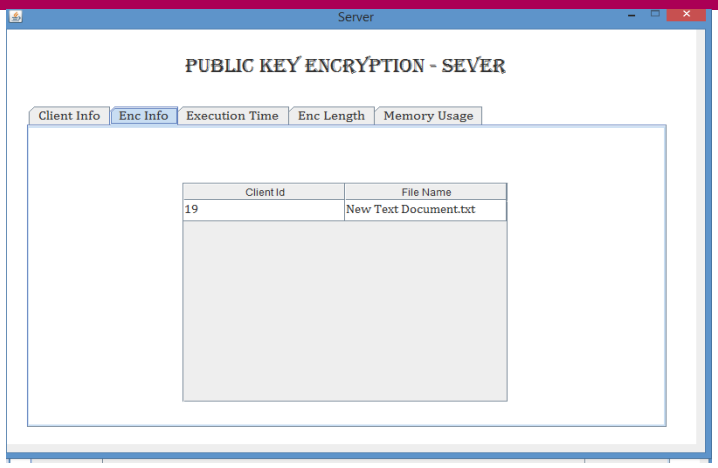

Figure 6Encryption information

3.3 Group Key Generation within the Workgroup

The hubs in the workgroup will frame a gathering key. Each gathering part will cooperatively contribute its part to the worldwide gathering key. The gathering key is created in a common and contributory style and there is no weak link. we will produce a gathering key. The gathering individuals are organized in a sensible key order known as a key tree. In the appropriated key arrangement conventions we consider, nonetheless, there is no concentrated key server accessible. In addition, a benefit of conveyed conventions over the concentrated conventions is the expansion in framework dependability, on the grounds that the gathering key is produced in a common and contributory style and there is no single-point-of-failure. To productively keep up with the gathering key in a unique friend bunch with multiple individuals, we utilize the tree-based bunch Elliptic Curve Diffie Hellman convention. Every part keeps a bunch of keys, which are organized in a progressive parallel tree.

Figure 7Key generation

3.4 Sharing Data within the Workgroup

With the assistance of gathering key created by the individuals in the gathering, the information will be shared safely among the gathering. The gathering individuals will share the assets, specifically getting to the documents. We are executing this with RMI (Remote Method Invocation). This component supports building appropriated applications. A remote item is one whose techniques can be summoned from another Java virtual machine, possibly on an alternate host. An object of this sort is portrayed by at least one far off interface written in the Java programming language. A reference to a remote item can be passed as a contention or returned accordingly in some strategy conjuring.

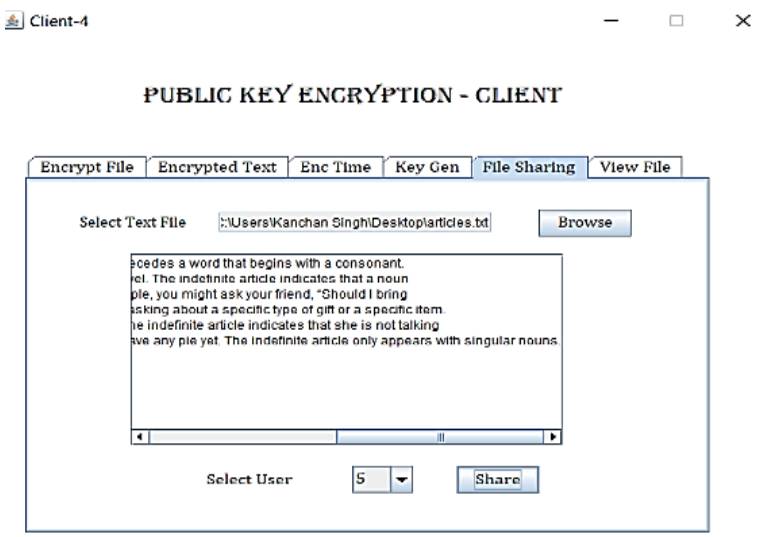

Figure 8File sharing

Figure 9View file

First of all, the client should login with epic client id, thereafter the user has to select the file for encrypting the data in the system. Four algorithms are used to encrypt the data, such as AES, RSA, DH and ECC. After encrypting the data, the key generation takes place, then key will be randomly generated. To share the encrypted data, select the client id and share the file to the receiver. The sender will pass the generated key for decrypt the encrypted data to the receiver. Finally, algorithms will represent the graphical representation of Time complexity, memory usage and length of the encrypted text.

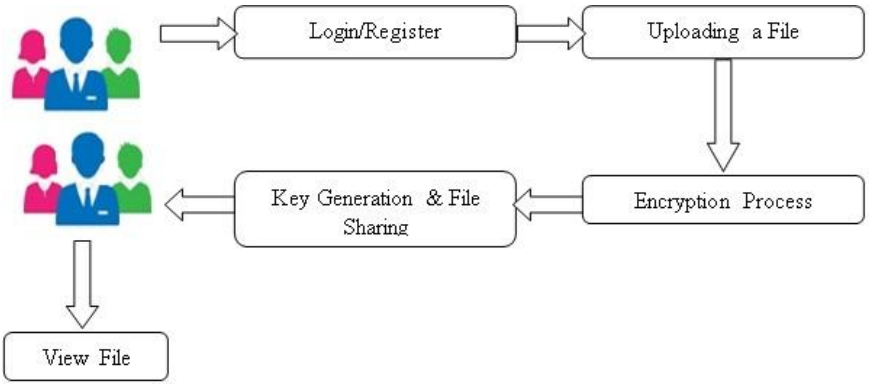

Figure 10Workflow diagram

4. Results and Discussions

The result showshave better Execution time, Memory usage and Encryption length. It minimizes the encryption length and encryption time and also occupies only small amount of memory. The mixture of four algorithms provides a greater security in cloud storage. The existing system's problem is resolved by using this method.

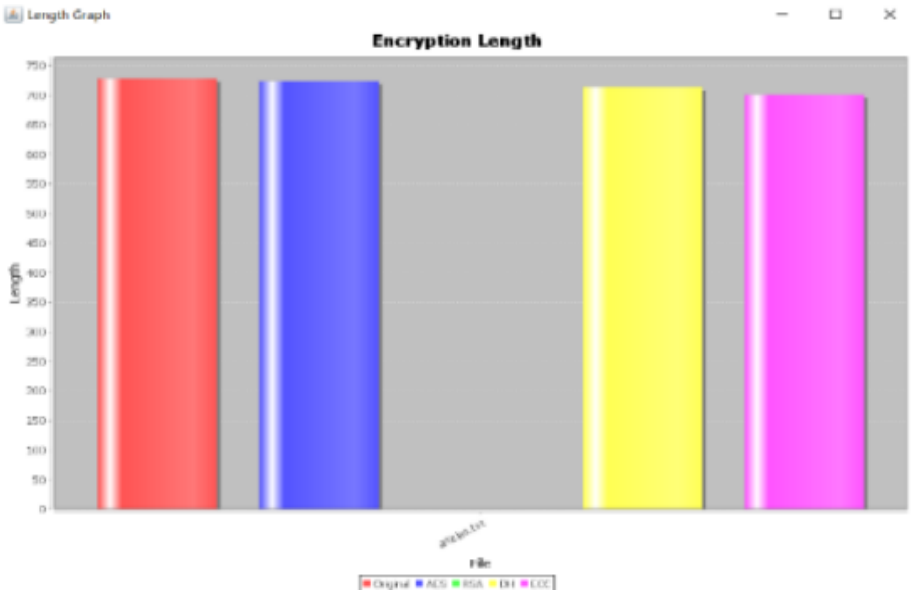

Figure 11Encryption length

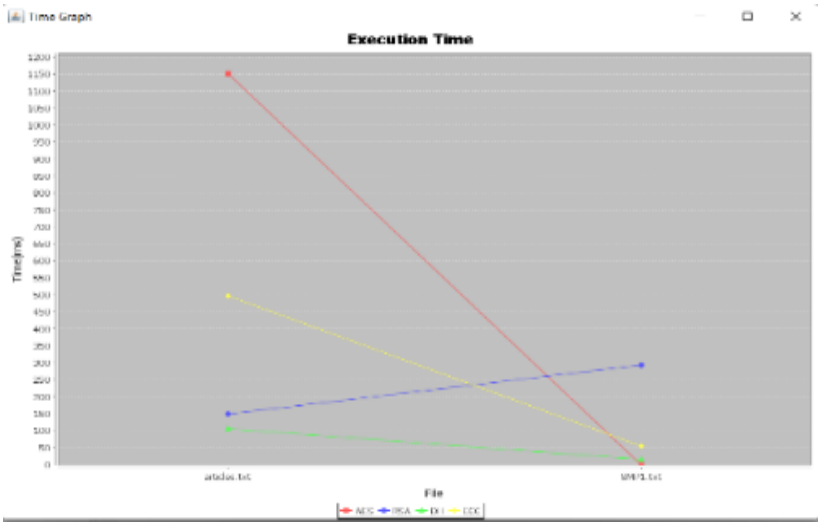

Figure 12Execution time

Figure 13Memory usage

5. Conclusions

The proposed project successfully overcomes the drawbacks of existing system. Combination of four algorithms provides better security than existing model. The Cloud processing as an innovation would be taken on assuming the areas of worries like security of the information will be covered. The strength of distributed computing is the capacity to oversee gambles specifically to security issues. Our proposed model will introduce a diagram sketch of design to be taken on by engineers engaged with executing the distributed computing. Security calculations referenced for encryption and unscrambling and ways proposed to get to the interactive media content can be carried out in future to upgrade security structure over the network.

The proposed framework investigates our work by giving calculation executions and delivering results to legitimize our ideas of safety for distributed computing. For this way to deal with fill in as planned, the cloud specialist organization must co-work with the client in executing arrangement. The proposed system was successfully completed and executed.

References

1. M. Aslam, C. Gehrmann, L. Rasmusson, and M. Bj ¨orkman,(2012), "Safely sending off virtual machines on reliable stages in a public cloud - an undertaking's point of view.," in CLOSER, pp. 511-521, SciTePress.

2. B. Blanchet,(2001), "An effective cryptographic convention verifier in view of prolog rules," in Computer Security Foundations Workshop, IEEE, pp. 0082-0082, IEEE Computer Society.

3. D. Dolev and A. C. Yao,(1983), "On the security of public key conventions," Information Theory, IEEE Transactions on, vol. 29, no. 2.

4. S. Graf, P. Lang, S. A. Hohenadel, and M. Waldvogel,(2012) "Adaptable key administration for secure distributed storage," Reliable Distributed Systems, IEEE Computer Society, pp. 469-474.

5. T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh, (2003),"Terra: A virtual machine-based stage for confided in figuring," in ACM SIGOPS Operating Systems Review, vol. 37, ACM.

6. S. Kamara and C. Papamanthou, (2013), "Equal and dynamic accessible symmetric encryption," in Financial Cryptography and Data Security, pp. 258-274, Springer.

7. Michalas, N. Paladi, and C. Gehrmann, (2014), "Security parts of e-wellbeing frameworks relocation to the cloud," in E-wellbeing Networking, Application and Services (Healthcom' 14), pp. 228-232, IEEE.

8. N. Paladi, C. Gehrmann, M. Aslam, and F. Morenius, (2013), "Confided in Launch of Virtual Machine Instances in Public IaaS Environments," in Information Security and Cryptology (ICISC'12), vol. 7839 of Lecture Notes in Computer Science, pp. 309-323, Springer.

9. N. Paladi, C. Gehrmann, and F. Morenius, (2013),"Domain-Based Storage Protection (DBSP) in Public Infrastructure Clouds," in Secure IT Systems, pp. 279-296, Springer.