Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

MODIFIED INTELLIGENT ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM TO MITIGATE SECURITY CONCERNS OF BIG DATA STORAGE IN MULTI-CLOUD ENVIRONMENT

V. L. PADMA LATHA
Research Scholar, Dept. of CSE, SVCE, JNTUA, Tirupathi
Dr. N. SUDHAKAR REDDY
Professor, Dept. of CSE, SVCE, Tirupathi
Dr. A. SURESH BABU
Professor, Dept. of CSE, JNTUACE, JNTU Anantapur

Abstract

A multi-cloud environment is created by combining many public and private clouds. In order to avoid vendor blockage, there are several cloud services that may cooperate and communicate with one another. Security and privacy of multi-cloud data are key concerns in cloud computing. Concerns about security and privacy abound since cloud service providers have access to sensitive data. In several areas, including banking and government, cloud computing adoption has been limited by this concern. To prevent cloud service providers from directly accessing the user's data, an intelligent cryptography solution is proposed in this study. According to the suggested strategy, sensitive material is divided into distinct files and stored on cloud servers based on relevance. To classify a file as sensitive or non-sensitive, the user selects the appropriate checkboxes. Virtual machines (VMs) are utilized to store sensitive information, and a single virtual machine (VM) is allocated to non-sensitive files. Elliptic Curve Integrated encryption Scheme (ECIES) is used to encrypt the data before uploading them to a cloud server. According to this research, ECIES cryptography can prevent cloud service providers from accessing customers' private information. The results of our trials reveal that our method is capable of fighting against the most frequent cloud-based attacks while still using a fair amount of processing time.

Keywords: Cloud Computing; Data Privacy; Security; Elliptic Curve Integrated Encryption Scheme; Sensitive Data; Virtual Machine.

1. Introduction

In the commercial phase of development, cloud computing technology is utilised. There are a wide variety of cloud service providers such as IaaS, SaaS and PaaS. In this scenario, users can utilise any service for any purpose. First, cloud computing was employed in conjunction with trade and university circles to create a hotspot for innovation. As a novel business representation model, it facilitates on-demand supply of computing and storage resources [1]. Trade is aided by providing software and services across the Internet to an enormous customer base via cloud computing services provided by commercial functions. The value of data to a company cannot be overstated. Data can be represented in a variety of ways, including numbers, phrases, graphics, and more. Businesses face a fundamental challenge when it comes to data isolation and protection. Data has a wide range of characteristics, including legitimacy, and consistency [2].

Nowadays, most of companies prefer the advantages of multiple clouds than single

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

cloud due to its flexibility and variety of services [3]. Rather than being open systems, many of today's public and private cloud networks are designed to run in isolation. In order to obtain the benefits of multi-cloud computing for companies, they must overcome the difficulties posed by the lack of interconnection between these networks .However,

Consumers must be secured in order to continue using their applications as usual after moving their data and applications to this multi-cloud approach. Customer account information is stored in the cloud by cloud service providers [4-5]. It is necessary for a customer to keep their passwords in several cloud services if they want to use multiple cloud services. For cloud service providers and their clients, the amount of copies of user data will be substantial, and security risks will increase. As a result, before moving data to multi-cloud, the organization must first classify it and then select the Cloud best suited to its requirements [6]. This distributed environment has led to a great deal of concern among enterprises regarding the security of their sensitive data and important applications in the cloud, as well as how to retrieve their data if something goes wrong[7].

Mass Distributed Storage (MDS) has also been used in recent years to increase the storage capacity [8-9]. MDS is considered an advantage because of its high-performance scalable processing. One area that requires improvement is the security of dispersed data storage [10], where threats originate from a various angles. For example, malicious attacks or abuse activities may be more likely to occur during data transports because of the distributed storage method [11-12]. As of right now, unanticipated actions can also occur on the cloud server side, which is mostly controlled by rules and regulations in most countries. Cost considerations make it challenging, however, to strike a balance between utility and security [13]. Consequently, securing dispersed data in cloud schemes is a complex problem since the hazards associated with multiple network levels are not fully addressed [14-15].

This study focuses on the topic of cloud operators abusing their power and preventing cloud users' data from being released from cloud servers. The ECIES concept, which stands for intelligent cryptography, is aimed to provide both an efficient MDS service and high-level security measures. It is our goal to encrypt all data and distribute it across multiple cloud servers without incurring large costs or delays. Our proposed solution aims to prevent cloud service providers from accessing consumers' source data directly. The paper's key contributions are two-fold:

- Cloud operators can't directly access users' original data through a proposed cryptographic solution we have developed. The cloud server's malicious activity can be protected using the cryptographic method suggested here.

- In this paper, we offer an efficient data splitting apparatus that does not generate large overheads, while also ensuring data retrievability.

The remainder structure of this paper follows as. Section 2 consists of existing techniques to solve the issues of cloud computing. The explanation of proposed methodology is provided in Section 3. The validation of ECIES with existing techniques is obtainable in Section 4. Finally, in Section 5 the conclusion is described.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

2. Literature Review

Confidential cloud digital signatures have been proposed by Pan et al [16]. Digital signatures are becoming increasingly used in the field of cyber security. As the verification of signatures is more time-consuming than the production of recall collated values. An elliptic curve digital signature technique (ECDSA) with a 256-bit key size is proposed in this research. Guess is a universal server for consecutively elliptic curve structures, and the algorithm runs on it. In order to increase throughput and computational capacity, Guess uses threads to implement. Subcontracting calculations for signature creation and authentication has been a common practice among defense practitioners. Guess uses additional software elements that can be readily upgraded and scaled. There is evidence in the study to support the claim that Guess may be used as a proof of secure network transactions, customizable features and optimization limits.

Cloud-based multimedia apps are becoming increasingly popular, according to Yang et al. [17]. In a cloud situation, such information can be saved, processed, and restructured in a cost-effective and structured manner. Although cloud computing services have security and protection concerns, the video content in a pool of clusters is recognised for a given time period in this work. All of the video content will be encrypted for only one user at a specific moment. There are additional suggestions for an efficient and effective method of updating consumer features, such as giving up innovative features, repealing previous features and grinding features that are previously repealed. New features can be signed and old ones revoked as part of the dynamic changes in user options.

Data encryption has been introduced by Amalarethinam and Leena [18]. RS Algorithm's asymmetric key sizes are the primary focus of this study. In order to ensure security, the file is divided into blocks of varying sizes. According to the block sizes, the suggested algorithm's key size is likewise increased to match the key size.

For the safe and efficient storage and sharing of sensitive personal data, the authors of paper [19] describe the "CHARON" cloud storage system, which makes use of numerous cloud providers and storage repositories. It doesn't necessitate any client-managed servers, and it effectively manages massive files on a geographically scattered storage set because of CHARON's three unique qualities. As a result, using byzantine-resistant cloud storage has the disadvantage of a higher latency, but the adding of a biometric identification system can be more actual in terms of security. In [20], worker nodes with various resources from multiple cloud providers can be used to increase the infrastructure's cost efficiency and ensure high availability by using a grid engine on top of a multi-cloud virtual environment. Oracle grid engine is used to distribute jobs to worker nodes that have been scheduled (in-house and cloud). When a job is sent to the Oracle grid engine master node, the worker nodes act as listeners. The grid gain engine receives the job from the Client following a valid authentication process. Hackers pose a serious threat, so access management is critical. Someone who has been granted access to the Cloud can be a potential hacker. Confidentiality of location data is a problem, which is solved by the authors of [21]. Structured multi-

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

level query tree is built to present the grouping of location data and access frequency, and then noises are added to the query tree nodes, which can increase protection location data.

2.2. Mass Distributed Storage (MDS)

Big data storage in cloud schemes is handled by MDS, one of the most common cloud computing approaches. In addition to security considerations, there are questions about storage availability, reliability, and accessibility when employing this method. A large amount of data makes the system integrations more difficult. Using MSD raises a number of security issues [22, 23]. Cloud-based MDS presents a number of significant challenges and opportunities, as stated below:

Data synchronizations face a major problem because of the limited computational resources available. If you're using large data, you should be able to have good synchronisation for users of various sizes. However, as the number of big data consumers grows, the computational resources are put under tremendous strain. This issue has been the subject of recent studies. In neural systems with asynchronous spiking, for example, a strategy [24] has been proposed to utilise the concept of local synchronisation. Using this method, distributed parallel computing devices can get the most out of their available processing power.

Many previous studies have examined, how cloud big data storage strategies can be used in practise to enhance business processes [25-26]. Research on information safeguards, such as access control systems and trust management, is another area of interest. To secure community data, for example, a trust level classification methodology has been developed [27]. If the trust communication setups for Instant Social Networking (ISN), this technique worked well for users [28]. An ontology-based authentication categorization system is presented in another recent research [29] for safeguarding multimedia data in cloud computing. The majority of these studies focused on safeguarding data transfer and authenticating users. There is little control over how data is stored when it is on the cloud.

In addition, encryption-oriented approaches to data protection on cloud servers are sought. Previous studies have also looked at this area, such as Fully Homomorphic Encryption (FHE) [30] and ABE [31]. Data can be efficiently protected against external malicious acts and internal incorrect operations using these types of safe techniques; but, the additional computations they require can have a severe influence on the efficiency of data processing. Noises in FHE make it impossible to carry out some tasks.

For the most part, there are two options for dealing with cloud-side data abuse. Restricting employees' behaviour through regulatory compliance procedures is the first step. Despite the best efforts of technical methods, this type of paradigm is difficult to manage. The use of encryptions like FHE and ABE, which prevent data from being leaked, is another option. However, this sort of data protection does not meet the needs of most modern industries because of its reduced operational efficiency and unresolved issues. A higher level of security is needed for large data-related

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

applications, thus we've come up with a novel approach to this problem.

2.3. Problem Identification

Cloud storage presents a wide range of security concerns. When it comes to cloud storage, consumers are most concerned about protecting their personal information. In the cloud, data storage is popular, but securing it is a difficult challenge for service providers to accomplish. Providers encounter a number of issues that are listed below.

❖ Individual data storage is critical in a cloud computing environment that is private and secure. In a variety of circumstances, the suppliers are defending customer data from the unknown.

❖ It is also indicated that data derivation for delivering counterfeit and non-repudiation is protected.

❖ Consumer fear of hacking, both inside and outside of the company. Encrypting all data without taking into account its privacy degree is a possibility.

3. Proposed Methodology

System Model

Figure 1 depicts a multi-cloud data storage scheme with three distinct entities.

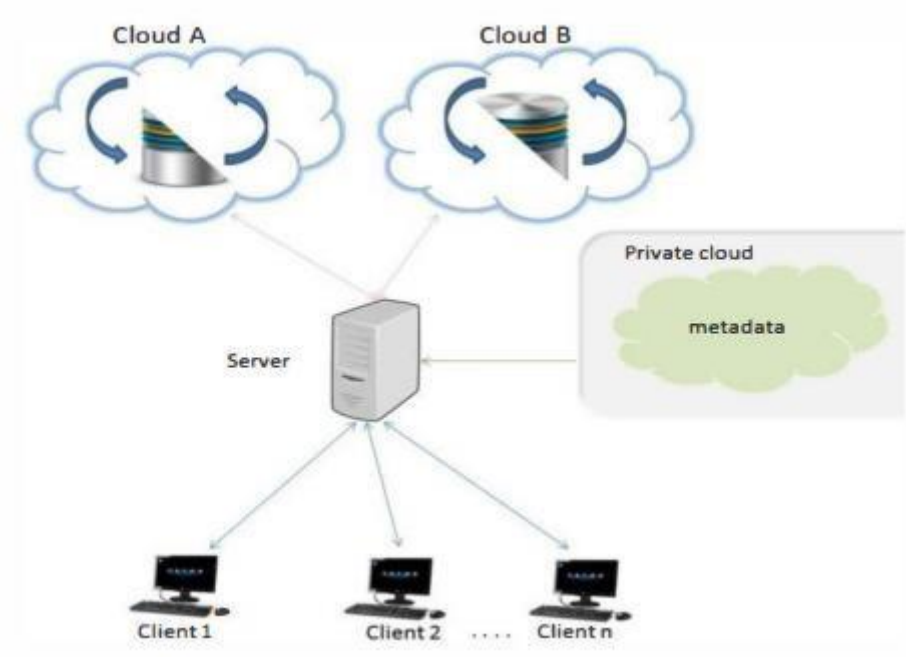

Figure 1: System Model

The following is a list of three distinct network entities:

❖ Users (US): People who have a huge amount of data files to store in multiple cloud providers.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

❖ Multiple cloud storage servers (CSSs) delivered by diverse cloud service providers with important computing power and storage space.

❖ A third-party auditor (TPA) who can certify the integrity of cloud data on behalf of cloud users.

A cloud storage server Organizer (O) is used to handle the interactions between the TPA and various CSSs, and each CSS is responsible for storing and maintaining a portion of users' data on its own. Organization and TPA can only communicate with each other via CSSs. The TPA and various CSSs are considered as semi-trusted entities by US. Consequently, we must safeguard data privacy while ensuring that the honesty of data stored in the cloud can be reliably validated.

As a first step, a customer requests a file storage space to the cloud service provider (CSP). If the file is a blank one, they'll look at the cloud server's storage capacity and accessibility. Then, the user will be able to regulate whether the input file is crucial or sensitive. Assuming it's a sensitive file, it will be split into multiple VMs, and if it's a non- sensitive file, it will be kept in one single virtual machine. Our algorithm is designed to maintain the encryption process that is necessary for restitution. The data is encrypted if it is stored on a cloud server by the data owner. An algorithm called ECIES is used to encrypt the data at this moment. Figure 2 depicts a generic block diagram of the proposed process, while a supplementary segment provides more specific details.

The proposed method is implemented in the following manner:

Step 1: Registration

Initially, users must create an account by providing an email address and a unique username/password combination. For the purposes of encryption, a password entered by the user is viewed as a private key. This private key is used in conjunction with the public key to encrypt the file. To decrypt the file, the same private key must be used.

Step 2: Key Generation

To put it another way, ECIES is a public-key system that provides authenticated encryption, and key exchange. As part of an Elliptic Curve Cryptosystem, the private key of an Elliptic Curve is used to encrypt information, and the public key of an Elliptic Curve is used to decrypt it. Even though implementation and design of public-key schemes might be a challenge, they are a vital means for securely exchanging information. In order to provide more secure authentication, key generation, key exchange, and key transmission techniques using less bandwidth on a network via a cloud server. Selecting an elliptical curve using the ECIES is useful when we wish to sign without using our private key, although we can also use the technique to encrypt data with our public key.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

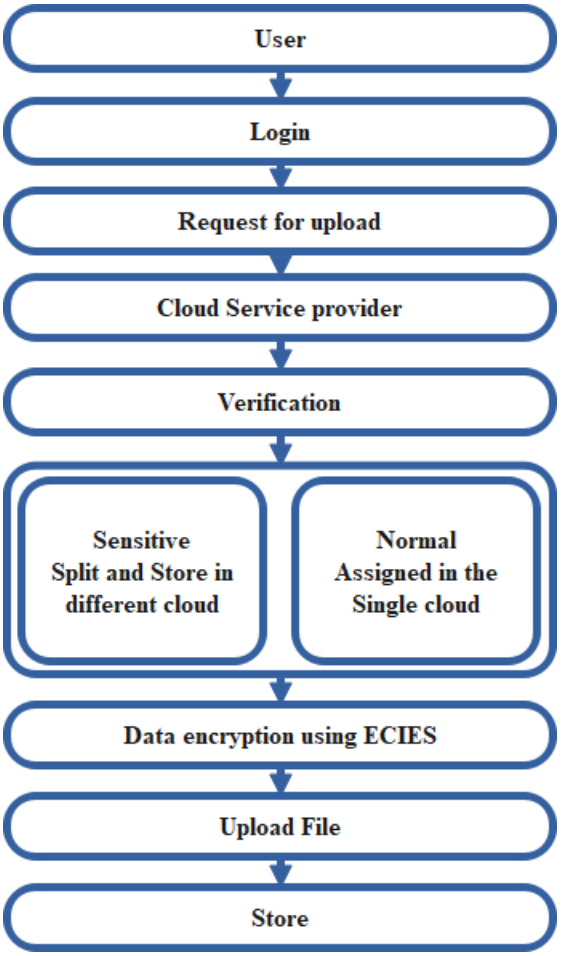

Figure 2. Proposed cloud computing cryptography-based data storage.

Step 3: Verification of File

Afterwards, the file's status is determined.

3.1. Normal File

The file will be handled in a single virtual machine if it is designated as non-sensitive.

3.2. Sensitive File

Files will be divided into various pieces dependent on the size of the data, if it is a sensitive file. A random virtual machine (VM) is assigned to each part of the data. All of our VMs can handle any number of files at once.

Step 4: Data Encryption using ECIES algorithm

The ECIES technique is used to encrypt packets in the mobile nodes before they are sent to the cloud server. Using the Secure Hash [31], it is used to store data and signatures from users. Encryption, digital signatures, and key exchange schemes are all provided by ECIES, which is a public-key method. To ensure safe authentication,

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

key generation, and key exchange procedures, Elliptic Curve (EC) uses smaller key sizes, which reduces the amount of bandwidth needed to transfer keys across a network through a cloud server [32].

Encryption using the ECIES: While the approach of selecting a curve is commonly used for key exchanges (signing with our public key and then proofing with our secret key), it may also be utilised for data encryption. Some of the fundamentals of elliptic curve cryptography are covered here. Assuming that we start with the public key of an x-y point, we can then use it to generate our private key, which is a random number that represents the gradient of the line leading from G.

$$Q = P.g \quad (1)$$

If you use prime Y large integer for finding the value of P in oval, it is really difficult even we have the value of Q and G. The equation for elliptic curve cryptography is given below:

$$y^2 = x^3 + ax + b \quad (2)$$

x and y are points on the curve's value, and a and b are the values of the points that define the curve. Here is how elliptic key encryption is implemented: The Integrated Encryption Scheme (IES) operates by generating a symmetric key from the public key of the recipient.

Elliptic curve (EC) will be used to generate public key pairs in the block chain implementation. An ECC algorithm that uses 256-bit public keys and is more secure than RSA's 3072-bit scheme. As with RSA, the elliptic curve uses smaller key sizes for equivalent security. Reduced key size and rapid processing speed are the primary advantages of employing EC-based cryptography security.

This is the procedure for creating the ECIES algorithm keys. It's the sender's responsibility to construct a random private key $RP_A * G$and then to find the sender's public key $P_A * G$on an elliptic curve.

$$PK_A = RP_A * G \ \ and \ \ PK_A = P_A * G \quad (3)$$

.

$$S = RP_A * R \quad (4)$$

The secret key generated by the receiver is exactly the same as the secret key generated by the sender.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

Step5: View File

$$RP_A * (R * G) \quad (5)$$

$$S = r * (RP_A * G) \quad (6)$$

$$S = r * PK_A \quad (7)$$

The suggested model is decrypted using the same key that was used to encrypt it.

Step 6: Accessing File

The file will be retrieved from the various cloud services in the sequence in which they were uploaded to the system.

Step 7: Display File

Decryption into plain text will be the final step.

3.2. Threat models

Numerous cloud service ideal designers presume that the cloud-side operators are secure because of the trustworthiness of the cloud server. However, rather than intentional attacks, many hazards are triggered by cloud operators' unanticipated actions. In many cases, although encryptions are used, data are still vulnerable. A tremendous deal of information can be leaked if harmful operations are allowed. As a result, we conclude that cloud operators are the primary source of dangers and construct two threat models based on current cloud activities.

1. ***Anti-Regulatory Compliance Threat (ARCT) Model:*** Cloud-side workers are assumed to have a desire to bypass the regulations and gain access to the data that are considered in this approach. Employees working in the cloud have access to the server and the encryption key.

2. ***Malicious Access Threat (MAT)****:* In this scenario, we adopt that the cloud-side operators seek to acquire harmful access to the data and information. The cloud server's data is saved in the cloud operator's knowledge. Even if the data are encrypted, the operators can make educated guesses about what they include, therefore even if the encryption level is high, the data can be decrypted.

Definition 1 can be used to build these two threat models.

Definition 1: A key K to decrypt a cloud-based data packet D, as K → D. Suppose cloud operators use K to D without approvals from the data owner.

3.2. Design goals

In order to assurance the data security essential by specific data consumers, our suggested system intends to simultaneously meet a number of targeted performance goals as follows:

❖ Our goal is to attain a higher level of security data storage by splitting data across varied cloud servers.

❖ This technology is designed to safeguard data from external threats, such as

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

those launched by criminals or terrorists. During the transmission procedure, data must be encrypted.

❖ Significant efficiency data processing: Our scheme will also reduce latency by avoiding high communication and computation overheads.

4. Results and Discussion

In order to conduct the experiment, Cloud Sim was used. This version of Net beans IDE includes Java 8. An Intel Core i5 computer with 8GB of RAM is being used. To upload files, a Java-based GUI for cloud sim was created, and Cloud analyst was used to determine where data centres should be placed. Low-configuration machines will be able to run the final product. However, the outcomes will be ineffective, and the duration may vary depending on the system's functionality. Table 1 shows the comparative analysis of proposed model with existing cryptographic techniques such as AES and ECC in terms of encryption time and decryption time. Figure 3 shows the graphical illustration of proposed model for encryption time.

Table 1. Encryption and decryption time taken.

Technique	File size (KB)	Encryption Time (ms)	Decryption Time (ms)
AES	10	645	578
	20	815	632
	30	1187	845
	40	1390	1011
ECC	10	617	543
	20	789	614
	30	1034	866
	40	1345	987
Proposed-ECIES	10	563	395
	20	715	496
	30	893	632
	40	1201	846

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

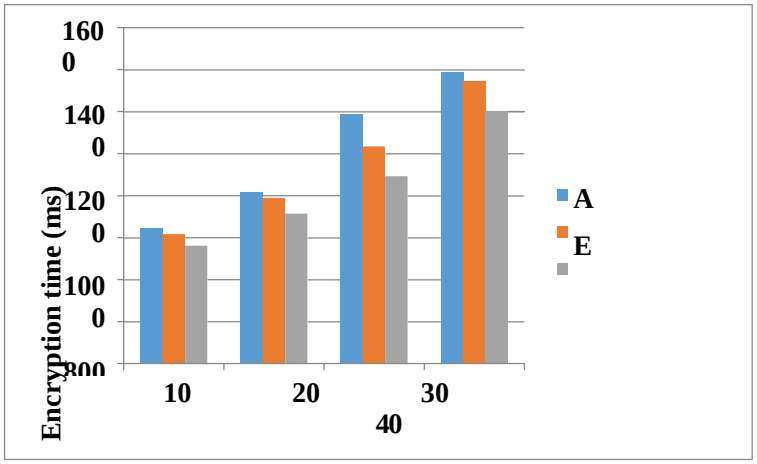

Figure 3: Graphical representation of proposed model in terms of encryption time.

When the file size increases, the encryption time is also increases. For instance, AES achieved 815ms, ECC achieved 789ms and proposed model achieved 715ms for the 20KB files. But, these same techniques achieved 1390ms, 1345ms and proposed model achieved 1201ms for the file size 40KB. This analysis proves that the proposed ECIES model has less encryption time than existing ECC and AES, even though the files are increased. Figure 4 shows the decryption time of proposed ECIES model.

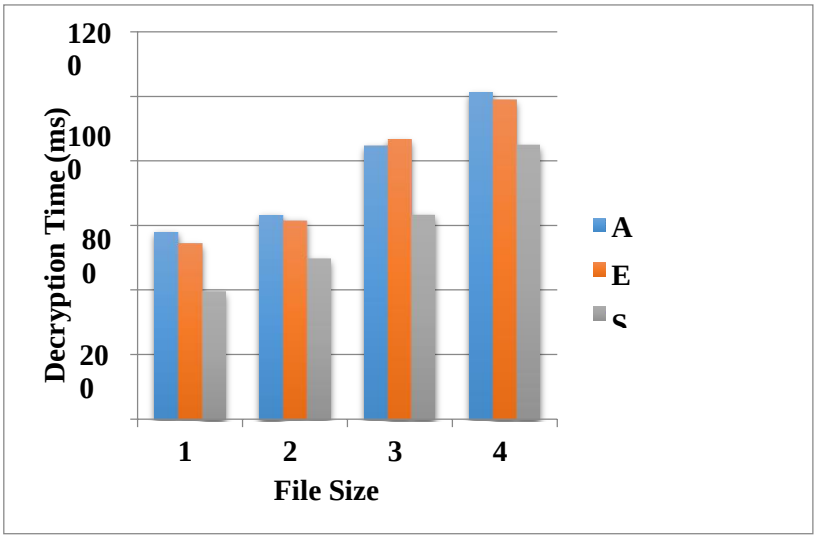

Figure 4: Graphical Representation of proposed model in terms of decryption time

When the file size increases, the decryption time is also increases. For instance, AES achieved 578ms, ECC achieved 543ms and proposed model achieved 395ms for the 10KB files. But, these same techniques achieved 845ms, 866ms and proposed model

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

achieved 632ms for the file size 30KB. This analysis proves that the proposed ECIES model has less decryption time than existing ECC and AES, even though the files sizes are increased. When comparing with encryption time, all models achieved less decryption time and the reason is that initially, the keys must be generated for files encryption and it will be easy for the same model to decrypt the files. Table 2 shows the comparative analysis of proposed ECIES model for uploading time and downloading time, where Figure 5 shows the uploading time of proposed ECIES model.

Table 2. Time taken for downloading and uploading time based on a file size.

Technique	File size (KB)	Uploading time (ms)	Downloading time (ms)
AES	10	3852	2984
	20	4671	3756
	30	5453	4290
	40	6814	5101
ECC	10	3917	2762
	20	4567	3841
	30	5740	4289
	40	6853	5574
Proposed-ECIES	10	2145	1465
	20	3365	2141
	30	4211	2965
	40	5236	3954

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

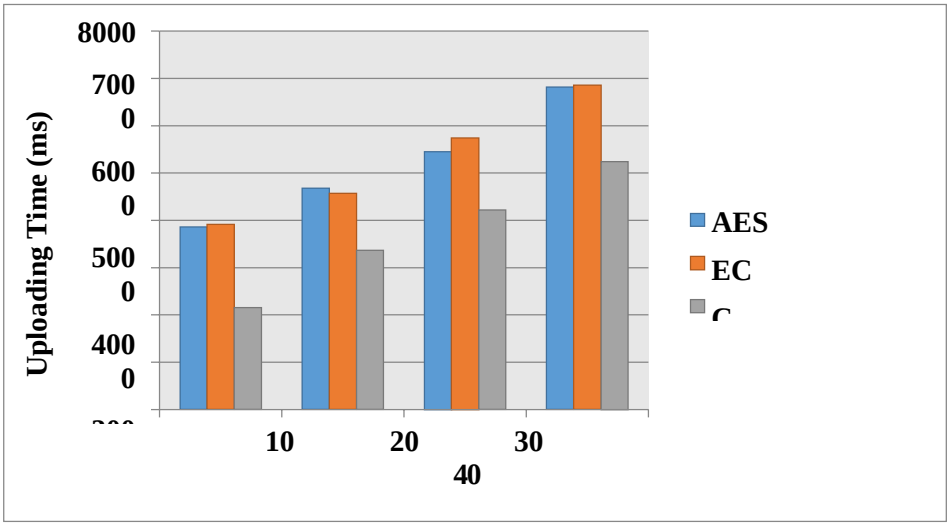

Figure 5: Uploading Time of Proposed ECIES model with existing techniques

The proposed model, AES and ECC techniques achieved high uploading time than encryption time and decryption time, because the uploading time is influenced by the file sizes. For example, when the file is 30KB, the AES and ECC techniques achieved nearly 5600ms and proposed ECIES model achieved only 4211ms. When the file size is less (i.e.10KB), AES and ECC techniques achieved nearly 3890ms and proposed model achieved only 2145ms. From this analysis, it is clearly proves that ECIES model has less uploading time than the existing techniques. Figure 6 shows the downloading time of proposed model with existing techniques.

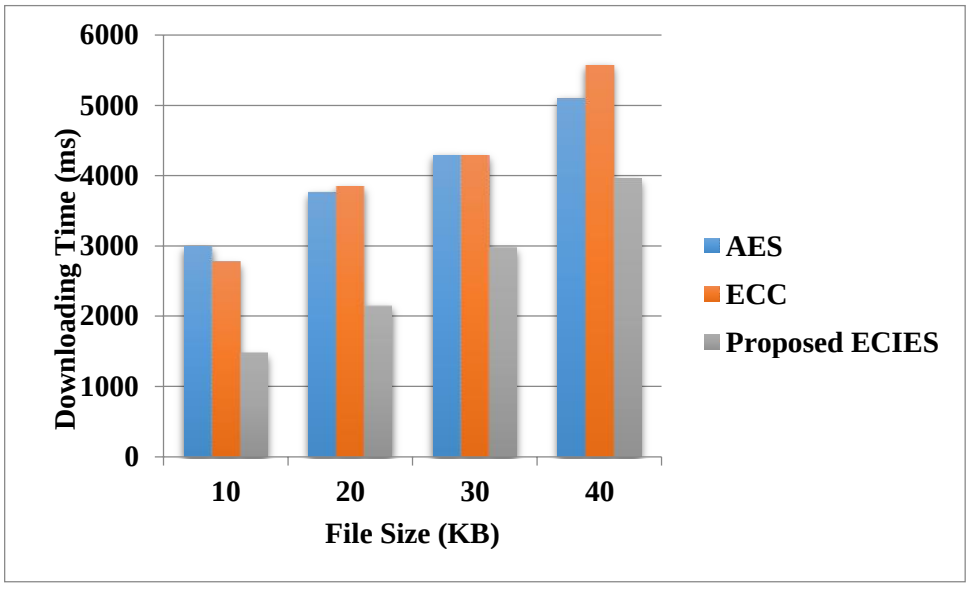

Figure 6: Graphical Representation of proposed model for downloading time with Existing techniques.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

The proposed model, AES and ECC techniques achieved less downloading time than uploading time. For example, when the file is 20KB, the AES and ECC techniques achieved nearly 3790ms and proposed ECIES model achieved only 2141ms. When the file size is high (i.e.40KB), AES and ECC techniques achieved nearly 5400ms and proposed model achieved only 3954ms. From this analysis, it is clearly proves that ECIES model has less downloading time than the existing techniques.

5. Conclusion

For this research, we sought to find a solution that would keep cloud service providers from accessing users' private data. We came up with an intelligent algorithm called ECIES to help us achieve this goal. Files are classified as either sensitive or non-sensitive by the user. If the file is vital to the user, then the ECIES algorithm is used to partition the file into smaller sections and store them in separate virtual machines (VMs). This information can be used to determine who made the changes to the evidence, which is very useful. It is thus possible to improve data dependability while respecting the privacy of user information. The JAVA platform is used to implement the algorithm in Cloud Sim. The results of the experiment show that the projected scheme performs better in terms of encryption and decryption time than the existing system. The experimental assessments had also shown that our proposed strategy could effectively protect against significant cloud-side dangers. Efforts to improve data availability will focus on safeguarding data duplications in the future, since data retrievals will fail if any of the data centres are unavailable.

References

[1] Xiao, Z. and Xiao, Y., 2012. Security and privacy in cloud computing. IEEE communications surveys & tutorials, 15(2),pp.843-859.

[2] Shaikh, R. and Sasikumar, M., 2015. Data Classification for achieving Security in cloud computing. Procedia computer science, 45,pp.493-498.

[3] Jignesh S (2017) The 6 multi cloud architecture designer for an effective cloud. https://simform.com/multi-cloud-architecture. Accessed 15 Apr 2018.

[4] Data integrity service in multi-cloud and distributed cloud storage environment. In: The 5th international conference on advanced computing and communication technologies. IEEE, India, p490–494.

[5] Megouache L, Zitouni A, Djoudi M (2018) A new framework of authentication over cloud computing. In: Silhavy R, Silhavy P, Prokopova Z (eds) Cybernetics approaches in intelligent systems. CoMeSySo 2017. Advances in intelligent systems and computing, vol 661. Springer, Cham, pp262–270.

[6] Travis W (2017) Five principles for running securely in a multi-cloud environment. https://threatstack.com/blog/5-principles-for-running-securely-in-a-multi-cloud-environment. Accessed 12 Nov2018.

[7] Tweaks C (2013) Importance of cloud computing interoperabilitiy. https://cloudtweaks.com/2013/10/importance-of-interoperability-providerlockin. Accessed 15 Nov 2018.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

[8] K. Gai, M. Qiu, H. Zhao, Security-aware efficient mass distributed storage approach for cloud systems in big data, in: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), IEEE, New York, USA, 2016, pp.140–145.

[9] H. Wang, Z. Xu, H. Fujita, S. Liu, Towards felicitous decision making: An overview on challenges and trends of big data, Inf. Sci. 367 (2016) 747–765.

[10] G. Ateniese, K. Fu, M. Green, S. Hohenberger, Improved proxy re-encryption schemes with applications to secure distributed storage, ACM Trans. Inf. Syst. Secur. 9 (1) (2006) 1– 30.

[11] J. Baek, Q. Vu, K. Liu, X. Huang, Y. Xiang, A secure cloud computing based framework for big data information management of smart grid, IEEE Trans. Cloud Comput. 3 (2) (2015)233–244.

[12] K. Gai, M. Qiu, L. Tao, Y. Zhu, Intrusion detection techniques for mobile cloud computing in heterogeneous 5G, Secur. Commun. Netw. (2015)1–10

[13] G. Wu, H. Zhang, M. Qiu, Z. Ming, J. Li, X. Qin, A decentralized approach for mining event correlations in distributed system monitoring, J. Parallel Distrib. Comput. 73 (3) (2013) 330–340.

[14] M. Qiu, M. Zhong, J. Li, K. Gai, Z. Zong, Phase-change memory optimization for green cloud with genetic algorithm, IEEE Trans. Comput. 64 (12) (2015)3528–3540.

[15] K. Gai, M. Qiu, H. Zhao, L. Tao, Z. Zong, Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing, J. Netw. Comput. Appl. 59 (2015)46–54.

[16] Pan, W., Zheng, F., Zhao, Y., Zhu, W.T. and Jing, J., 2016. An efficient elliptic curve cryptography signature server with GPU acceleration. IEEE Transactions on Information Forensics and Security, 12(1),pp.111-122.

[17] Yang, K., Liu, Z., Jia, X. and Shen, X.S., 2016. Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach. IEEE Transactions on Multimedia, 18(5),pp.940-950.

[18] Amalarethinam, I.G. and Leena, H.M., 2017, February. Enhanced RSA algorithm with varying key sizes for data security in cloud. In 2017 World Congress on Computing and Communication Technologies (WCCCT) (pp. 172-175).IEEE.

[19] Qamar N, Ana S, Eran E (2018) Securing DICOM images based on adaptive pixel thresholding approach, computerbased medical systems (CBMS). In: IEEE 31st international symposium pp280–285.

[20] Ricardo M, Tiago O, Vinicius C, Nuno N, Alysson B (2019) CHARON: a secure cloud- of-clouds system for storing and sharing big data, In: IEEE transactions on cloud computing p 19–39.

[21] Gu K, Yang L, Yin B (2018) Location data record privacy protection based on differential privacy mechanism. Inf Technol Control47(4):639–654.

[22] C. Chen, M. Won, R. Stoleru, G. Xie, Energy-efficient fault-tolerant data storage and processing in mobile cloud, IEEE Trans. cloud comput. 3 (1)(2015)

28–41.

[23] Y. Li, W. Dai, Z. Ming, M. Qiu, Privacy protection for preventing data over-collection in smart city, IEEE Trans. Comput. 65 (5) (2016) 1339–1350.

[24] T. Song, L. Pan, G. Paun ˘ , Asynchronous spiking neural P systems with local synchronization, Inf. Sci. 219 (2013)197–207.

[25] M. Cimino, F. Marcelloni, Autonomic tracing of production processes with mobile and agent-

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:03:2022
DOI 10.17605/OSF.IO/N6Z7U

based computing, Inf. Sci. 181 (5) (2011)935–953.

[26] Z. Yan, Y. Chen, Y. Shen, A practical reputation system for pervasive social chatting, J. Comput. Syst. Sci. 79 (5) (2013)556–572.

[27] Z. Yan, M. Wang, P. Zhang, A scheme to secure instant community data access based on trust and contexts, in: IEEE International Conference on Computer and Information Technology, IEEE, Xi'an, China, 2014, pp. 646–651.

[28] Z. Yan, P. Zhang, A. Vasilakos, A survey on trust management for internet of things, J. Netw. Comput. Appl. 42 (2014)120–134.

[29] Y. Li, K. Gai, Z. Ming, H. Zhao, M. Qiu, Intercrossed access control for secure financial services on multimedia big data in cloud systems, in: ACM Transactions on Multimedia Computing Communications and Applications, 2016, p.1.

[30] T. Plantard, W. Susilo, Z. Zhang, Fully homomorphic encryption using hidden ideal lattice, IEEE Trans. Inf. Forensics Secur. 8 (12) (2013)2127–2137.

[31] M.K. Pandya, S. Homayoun, A. Dehghantanha, Forensics investigation of openflow- based SDN platforms, Adv. Inform. Security 70 (2018)281–296.

[32] Y. Xie, D. Feng, X. Liao, L. Qin, Efficient monitoring and forensic analysis via accurate network-attached provenance collection with minimal storage overhead, Digit. Investig. 26 (2018)19–28