Journal, Advances in Mathematical & Computational Sciences
Vol. 10 No.4, December, 2023
www.isteams.net/mathematics-computationaljournal

Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD) USA

Available online at https://www.isteams.net/ mathematics-computationaljournal.info
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

Secured Data Transmission Using Elliptic Curve Cryptography.

Murphy, B.B., Mitana, O.H & Obanor, P.
[1]Department of Computer Science, Niger Delta University, Bayelsa State, Nigeria.
[2,3]Deprtment of Physical Sciences, Benson Idahosa University, Edo State, Nigeria
Emails: tukamurphy@ndu.edu.ng; amitana58@gmail.com; pobanor@yahoo.com

ABSTRACT

Cloud Computing is described as the next-generation architecture of IT Enterprise which facilitate data transmission among the server and client. Cloud computing afford organizations cost savings and operational efficiencies with new security risks and uncertainties. The increased attacks in a Cloud environment allows for other vulnerabilities to be exploited, thereby increasing the organization's risk. As a result of data sensitivity in applications, platforms and infrastructure, cloud security poses a major concern as a user within the cloud environment. The two major issues associated with the cloud are data theft and illegal access. Albeit these issues, we designed a public key cryptographic algorithm (ECC) to prevent any attacks during the transmission of data in the cloud. This study is important as it utilize the Elliptic Curve algorithm which has enhanced security services than RSA public key algorithm as a result of its elliptic curve theory.

Keywords: Cloud Computing, ECC, SHA-256, RSA, Cryptography.

Murphy, B.B., Mitana, O.H & Obanor, P. (2022): Secured Data Transmission Using Elliptic Curve Cryptography.
Journal of Advances in Mathematical & Computational Science. Vol. 10, No. 4. Pp 1-10.
Available online at www.isteams.net/mathematics-computationaljournal.

1. INTRODUCTION

Cloud computing represents a major change in how information is being stored and transmitted from the client to the server and vice versa. Instead of hosting data on individual computer and servers, these data are stored in the cloud. Over 80% of business executives are full of excitement due to the benefits of utilizing the cloud service but 80% are scared on security, availability and privacy of these stored data and how client can transmit the data to the server without any form of attack.

Cloud Computing is a tidal wave in IT Enterprise which enable the mobilization of application software and databases to centralized large data centers where the management of the data and services may not be fully trusted. However, security is a significant challenge which limit users from taking the full advantage in the usage of cloud computing services.

In order to achieve user's trust, data protection and security must be taken into cognizant. Consequently, (Karrar and Fadi, 2018), mentioned the concern of cloud service users in ensuring the safety of their sensitive data in insecure place. Although, data on the cloud faces problems such as theft and unauthorized access but to overcome these problems in the cloud, some security strategies need to be implemented. Similarly, (Theebendra and Santhini, 2014) developed an effective and flexible distributed scheme with two salient features to ensure the correctness of users data in the cloud. Moreover, several researches on protocols that helped to secure data during transmission have been carried out. These protocols provide confidentiality, integrity, non-repudiation and authenticity of data (Karrar and Fadl, 2018). Due to technological advancements, blockchain and steganography techniques are evolving in solving these security issues.

Additionally, cryptographic encryptions have been applied to substantiate data confidentiality; hash function to confirm data integrity and digital signature for authenticity and non-repudiation using several cryptographic techniques. Cryptography is a process of converting data into a meaningless and unreadable form in order to shield it from unauthorized access, while maintaining the security of the data. The two major cryptographic algorithms are symmetric key based (private key) and asymmetric key based (public key). In this research, we proposed a public key encryption (Elliptic Curve Cryptography) for an enhanced security to prevent any attacks during client–server data transmission.

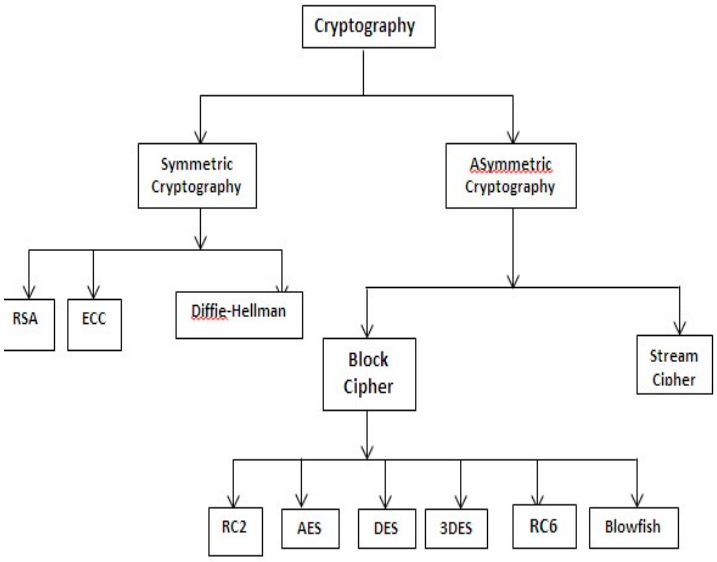

Figure 1: Classification of Cryptographic Algorithms.

2. RELATED WORKS

Devi et al (2016) proposed a secure data transmission in cloud computing. The study presented a cloud-based storage scheme where users can earn mutual trusts and maximize the benefits from the customer service provider (CSP) services. Four distinct features which enable the owners to outsource sensitive data to a CSP and perform operations such as insertion, deletion, append etc. on the data, ensures only authorized users access to the latest version of the outsourced data; enables indirect mutual trust between the owner and the CSP; and allows the owner to grant or revoke access to the outsourced data were analyzed. However, the authors did a good job but the study utilized a Trusted-Third-Party protocol which may not be able to provide total reliance and authenticity between the client and the server. Poduval et al (2019) implemented a secured cloud storage using hybrid cryptography mechanism. The study implemented 128-bit keys cryptographic algorithms such as 3DES, RC6 and AES cryptographic algorithms with steganography to provide enhanced data security. However, the steganography technique was utilized to secure key information, which contains details of encrypted file, the algorithm and its key.

Although, the study methodology provided an improved security of customer data using secret-key encryption methods but was unable to implement same with some public encryption techniques such as RSA, ECC etc, as this could help to eradicate further attacks during data transmission. Karrar and Fadi (2018) carried out a research on protocols for securing cloud data. The study make use of symmetric and asymmetric encryption mechanisms, hash function and digital signature in substantiating data confidentiality, integrity, authenticity and non-repudiation. However, the proposed design was able to provide those distinctive features of data but suffered some major drawbacks, such as inability to use Advanced Encryption Standard and a public key scheme like Elliptic Curve (EC). Jatauwycliff et al (2016) stated the need to make cloud environment safe and secure by addressing the security challenges within the cloud.

However, cloud providers employ encryption security measures which is inadequate but this study provided a detailed analysis on cloud data security and privacy protection at all stages of data life cycle. In contrast to the traditional method, which could not prevent unauthorized third party from gaining access to organizational data, cloud security became a major issue that must be tackled to ensure safety of global data. The authors did a good job but could not include enhanced security measures such as thumb-print, facial recognition, voice recognition and image identification for cloud data.

Kumar and Prakash (2020) proposed a 128-bit key encryption for file storage using hybrid cryptography. The study utilized some symmetric key encryption methods such as RC6, 3DES and AES and steganography technique for data and key information storage respectively. The proposed system was able to achieve the integrity, enhanced security, low delay, authentication, and confidentiality of data during transmission. Although the system could not be implemented to further detect any attacks during client-server data transmission using the researched public key cryptographic mechanisms. Chavan et al (2019) established a secured mechanism for authenticating data in a network using both symmetric and asymmetric algorithms, and OTP. OTP (One time password) is said to provide strong authentication while the AES and RSA algorithms provided strong encryption for the data.

However, the study focused on ensuring high security and performance of cloud computing by enhancing a mechanism for data transmission over the internet but lack architectural model on the discussed issue for more clarification in achieving the set goal.

Selvanayagam et al (2018) researched on using cryptography for secure file storage. The study aimed to ensure that cloud data are safe using elliptic curve encryption and only available with authorized access. Security and performance of cloud data were the major focus of the study. The ECC Encryption algorithm was utilized to provide high performance during encryption and decryption process. However, the authors discussed the various cryptographic techniques but were unable to implement the discussed issue to an architectural model for clarity of purpose. Madhumala et al (2021) designed a web-based cryptographic approach for data security. The proposed study discussed how certain issues regarding users' data can be handled by encryption rather than the traditional method of storing them in a plain form. This will help to prevent any attackers from reading, deleting and manipulating the data. In addition, the proposed model focused mainly on user authentication and security before storing and sharing files, in order to create an application that lets a user to encrypt and decrypt any type of file without any changes in the size, store every user data in the encrypted format, provides a communication medium between users through the chat application and afford direct access to the file. The authors did a good job but failed to include the encryption and decryption process on larger files.

2.1 Security Services In Cloud Computing

As a result of innate characteristics of the cloud, the need for enhanced security measures arise in order to provide sophisticated security to data during transmission and also boost trust among cloud users. However, adequate security services must be in place in order to enable potential users to securely and confidently move their applications to the cloud.

The following are security services available for information security:

- Confidentiality: This is an important security service that must be taken into cognizant in order to prevent illegitimate users from gaining access to the data. Besides, different applications differs in requirements in terms of confidentiality.
- Integrity protection: Once data are outsourced to remote cloud servers, it must be protected to avoid malicious modification of such data during transit. The integrity of data is a core value to cloud users and it is also critical to guarantee that all the audit data are authentic especially in legal consideration.
- Availability: Availability service ensure that the data stored in the cloud are available at users' request. This service is very vital mostly for data at rest in cloud servers, which is related to the fulfillment of Services Level Agreement. Although, for long-term data storage services, availability assurance is very necessary due to the increasing possibility of data damage or loss.
- Secure Data Access: This helps to put an end to the accessibility of data content to unauthorized users. In practical applications, disclosing application data to unauthorized users will help to treat the cloud user's main goal.

2.2. Cloud Data Transmission Security Challenges

Business organizations and executives have devised a means to save cost by providing support on the need to move organizational information to the cloud and this afford them access to global resources without much delay. However, this movement requires adequate security measures in order to protect client information from any security breach and leakage. Existing security challenges in data transmission are highlighted below:

a) Data Integrity

This maintain the consistency, accuracy and confidentiality of data by making sure that the online data are not mutilated and that only legitimate users can gain access to it either for usage and/or modification.

b) Insecure Access Control

Cloud services makes data or information to be available from any device rather than from a remote location. However, this has an inherent risks such that the interfaces and the application programming interfaces (APIs) can interact. Although, with are insecure access, hackers can exploit these vulnerabilities and authentication via APIs if given ample time.

c) DDoS and Denial-of-Service Attacks

The cloud environment is becoming bigger targets for attackers as more and more business processes are moving to the cloud. The need for enhanced security measures with constant update by cloud providers in order to combat this situation. As a result of technological growth, distributed denial of service has become more famous and designed to hijack website servers from legitimate requests. Upon a successful launch of DDoS, the website servers will be redundant for a long time, leading to revenue loss, breached trust and brand authorization. Therefore, it is very important to include DDOS protection technique in cloud services.

d) Data Breaches

An unauthorized access to data, theft, loss and dissemination of information is referred to as data breach. It may also include leakage of personal information such as credit card numbers, personal health information, personally identifiable information or corporate information like client list, source codes and intellectual property or business secrets. Since sensitive data are transported within an organization and a third party environment, the challenge of data loss, security and privacy cannot be overlooked. However, every organization is accountable for the usage, accessibility and security of their data by ensuring proper security measure for such data rather than leaving it solely for service providers to secure the data sent to the cloud. Despite various research directions in cloud service usage, the security policies and programs requires constant update and investigation for further improvements. Although, there are many reasons why data breach happens as analyzed by (Paudel, 2019) making reference to Identity Theft Resource Center.

Some of the common causes of data breaches are (Paudel, 2019):

- Hacking/Intrusion: This encompasses all forms of social engineering attacks such as Vishing, Smishing, Phishing and malware/ransomware.
- Web data exposure: Placing sensitive data on the web can expose them to all forms of attacks.
- Data on the Move: Most organizations find it very difficult to secure their data in transit. Utilizing HTTP and other protocols cannot guarantee adequate security of data during transmission form one client to another or client to server and vice versa.
- Employee Negligence: Weak and unenforced security policies such as employee negligence can result in unprecedented data breach.
- Inside-theft: Staff of an organization can intentionally breach data by exposing such data to cyber attackers.
- Physical-theft: Laptops and mobile devices used to store sensitive or valuable data can be lost or stolen.
- Illegitimate Access: Unauthorized users can gain access to sensitive data due to poorly designed access controls.

3. SYSTEM ARCHITECTURE

The existing system implemented secure data file model using steganography technique and symmetric cryptographic algorithms such as Triple Data Encryption Standard, Rivest Cipher 6 and Advanced Encryption Standard for cloud data security and encrypted file storage respectively. The existing approach splits the file into three equal parts during encryption with individual parts encrypted with different encryption algorithm and multithreading technique.

The steps includes:

a. Registration of the user: The user must first register themselves on the cloud in order to afford him access on cloud services. The registration process allow users' to enter their usernames, passwords, email ids and phone numbers so that the server can generate unique keys for encryption and decryption purposes. Steganography algorithm encoded with the user's profile picture will be used to store the unique key.
b. File upload: The uploaded file was first stored in a temporary folder and splitted into three different parts with different algorithms.
c. File download: Upon a user's request, the file will be downloaded and sectioned into three parts using the same encryptions algorithms to decrypt the file.

3.1 Proposed System

The proposed system utilize Elliptic Curve Cryptography (ECC) for cloud data transmission. This model will provide better data security due to the small key size and simplified computation. Elliptic curve applies the unique property of elliptic theory in encrypting data during transmission and used as an asymmetric key infrastructure. The fundamental calculation of ECC is regarded as point multiplication which involves the fundamental increase of a scalar K with any guide P on the curve towards another point Q on the same curve.

Generally, elliptic curve is expressed mathematically below:

"$y^2+axy+by = x^3+cx^2+dx+e$" where real numbers are a, b, c, d and e, while x and y represents set of real numbers. Simplified, thus; the elliptic curve equation is represented below:

'y^2-x8+dx+e' .....(1)

The system allow users to upload and request data in the cloud. The file is stored in the encrypted form and access is granted only to the authorized user(s). The proposed system accepts any kind of data for processing. Firstly, it accepts data from the user and utilize the cryptographic algorithm to generate the cypher text of the data.

The system advantages include:

1. secure file transfer using asymmetric algorithm.
2. the implemented cryptographic technique reduces space and time complexity by compressing the cloud data.
3. data integrity validation using SHA256 and ECC derivative.

In elliptic curve or public-key cryptosystem mechanism, every user has a public and a private key which is utilized for encryption/signature verification and decryption/signature generation respectively. However, the proposed system consist of three modules: **User, Administrator and Data Provider.** The user requests data from the cloud through the administrator by using his username, password and email id. The administrator verifies the user's request and provides the key; both the data and the key are encrypted and stored in the cloud. In the data provider module, the data undergo two steps before storage; firstly, SHA-256 will be used to get the sum value by passing the data content through the algorithm; secondly, the data will be passed through ECC as input. The generated cipher text will be encrypted and the secret key will be utilized to decrypt the encrypted key and shared to the user by requesting to the administrator.

Similarly, assuming two cloud users (A and B) wants to send data securely to each other such that A want to send data to B's cloud securely. The study applied digital signature and ECC encryption to securely transfer the data from A to B. For instance, if B wants a document from A's cloud, then B is expected to place a request to A. A will process B's request and apply SHA-256 hash function, to generate the message digest. The message digest will be digitally signed with A's private key by using A's software. B's public key and ECC algorithm will be used to encrypt the digitally signed signature. Therefore, the encrypted cipher message will be sent to B. However, B's software will decrypt the cipher message to word document using the private key and confirm the signature with A's public key.

Journal, Advances in Mathematical & Computational Sciences
Vol. 10 No.4, December, 2023
www.isteams.net/mathematics-computationaljournal

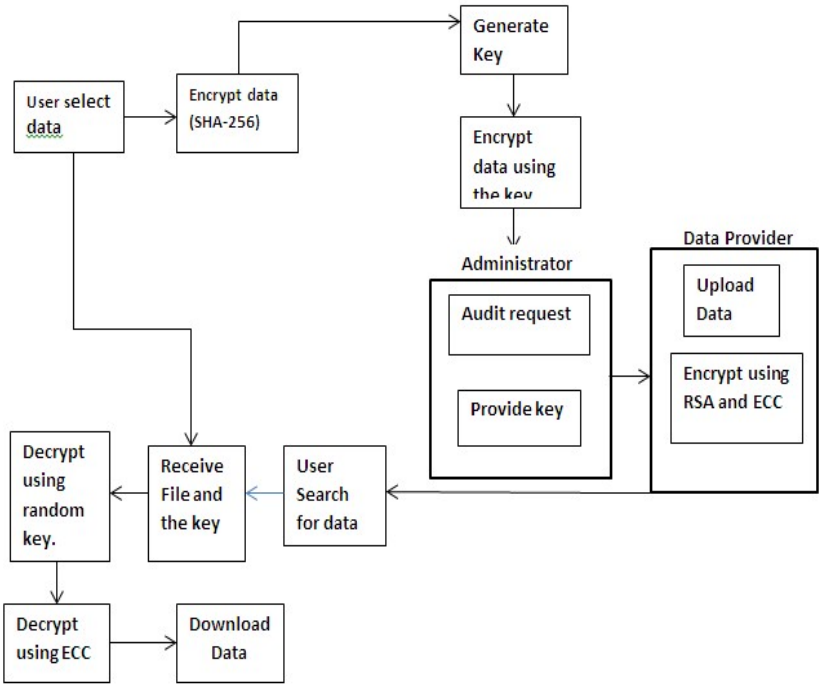

Figure 2: Proposed System Architecture.

Mathematically, the cryptographic mechanism involves five stages:

Key Generation

1. dA (Integer) represents A (private key)
2. PA=dA*B represents A(public key)
3. dB= B (private key) such that the public key is given as PB= dB *B
4. Compute the security key for A, such that
   K= dA *PB.
5. Compute B secret key such that
   K= dB *PA.

Signature Generation:

Pocedures for signing a message(m) by the sender (cloud A) using its private key dA is given as:

1. Given e= SHA-256 (m), where SHA-256 represents a cryptographic hash function.
2. get random integer z from (1, n – 1)
3. take r = x_1 (mod n), where
   (x_1, y_1) = z * B. If r =0, else goto step 2.
4. take s = z − 1(e + dAr)(mod n); If s = 0, else goto step2
5. The signature is taken as pair (r, s)
6. Send digital signature (r, s) to cloud B.

Data Encryption Process

For cloud 'A' to securely send a message to cloud 'B'; thus:

1. Cloud 'A' encodes a plain message onto a point, PM, from the elliptic group.
2. 'A' also chooses another random integer, z from the interval (1, p-1)
3. The cipher text is a pair of points given as PC = {(zB), (PM + zPB)}
4. The computed cipher text, PC, is sent to cloud 'B'.

Data Decryption Process

Cloud 'B' will decrypts the ciphertext sent by cloud 'A'; thus:

i. dB * (zB)= (Product of the first point from PC and his private key).
ii. Subtracts the product from the second point from PC such that [(PM + zPB) – (dB(zB)] = [PM + z(dBB) – dB(kB)] = PM.
iii. Cloud 'B' decrypts 'PM' to get the message digest (m).

Signature Verification

With cloud 'A' public key (PA), 'B' can confirm A's signature. Thus;

1. confirm that r and s are integers in (1, n – 1). Else, signature=invalid
2. calculate e = SHA-256(m), where SHA-256 is the same function used in the signature generation.
3. given w = s −1 (mod n)
4. given u_1 = ew (mod n) and
   u_2 = rw (mod n)
5. compute (x_1, y_1) = u_1B + u_2PA
6. valid signature = x_1 = r(mod n), else invalid.

4. CONCLUSION

The study utilized the Elliptic Curve Cryptography with greater security, efficiency, performance and bandwidth than the Rivest Shirman Adleman (RSA) technique. Consequently, ECC has proven to require less overheads than other asymmetric techniques with widespread usage in the near future. Although ECC provides same security relevance like the RSA with limited keys but lack sufficient research directions for easy understanding of the underlying mathematics.

However, in the future, ECC might have a better usage than RSA especially in recent applications such as smart cards, pagers, and cellular telephones and many more. Due to its smaller key size and less computing, ECC is constantly been used in today's small computing devices both for encryption and decryption, making it ideal for portable, lower power and mobile applications, integrating with cloud services. Further research studies will include comparing ECC with other digital signature algorithms, key exchanges and improved data integrity application in C2C communication.

REFERENCE

[1] Selvanayan, J., A. Singh, J., Michael and J. Jeswani. Secure file storage on cloud using cryptography.International Research Journal of Engineering and Technology (IRJET). 2018. 5(3). 2044-2047.

[2] Karrar, D.A.E and Fadi MFI. Security Protocol for Data Transmission in Cloud Computing. International Journal of Advanced Trends in Computer Science and Engineering. Jan-Feb 2018. 7(1). 1-5.

[3] Devi JS, R Aarthy, MSD Basha and AD Gnansekar. Secure Data Transmission In Cloud Computing. International Journal Of Current Research And Modern Education (IJCRME). 2016. 1(1). 141-146.

[4] Poduval A, Doke A, Nemade H, Nikam R. Secure File Storage on Cloud using Hybrid Cryptography. International Journal of Computer Science and Engineering. 2019. 7(1). 587-591.

[5] Jatauwycliff O, Abdulrahman S,Suleiman A. Enhancement of Data Security in Cloud Computing: Issues and Challenges. IOSR Journal of Computer Engineering (IOSR-JCE).Mar-Apr. 2016. 18(2). 12-17.

[6] Madhumala RB,Sujan C,Akshatha KC,Hitesh J. Secure File Storage & Sharing on Cloud Using Cryptography. International Journal of Computer Science and Mobile Computing. May-2021. 10(5). 49-59.

[7] Kumar U, and Prakash J. Secure File Storage on Cloud Using Hybrid Cryptography Algorithm. International Journal of Creative Research Thoughts (IJCRT). July 2020. 8(7). 334-340.

[8] Theebendra C, Santhini N. Cloud Computing Security - Data Storage and Transmission. International Journal of Research In Computer Applications and Robotics. Dec-2014. 2(12). 27-35

[9] Chavan A, Jadhav A, Kumbhar S, Joshi I. Data Transmission using RSA Algorithm. International Research Journal of Engineering and Technology (IRJET). Mar'2019. 6(3). 34-36.

[10] Selvanayagam J, Singh A, Michael J, Jeswani J. Secure File Storage on cloud using cryptography. International Research Journal of Engineering and Technology (IRJET). 2018. 5(3). 2044-2077.