A Secured Storage and Communication System for Cloud Using ECC, Polynomial Congruence and DSA

Nithisha J (nithisha.j@gmail.com)
Anna University Chennai

Jesu Jayarin P
Jeppiaar Engineering College

Research Article

Keywords: Elliptic Curves, Digital Signature Algorithm, Encryption, Decryption, Key Generation, Signature Generation, Signing and Verification.

Posted Date: October 25th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-824124/v1

A Secured Storage and Communication System for Cloud Using ECC, Polynomial Congruence and DSA

Nithisha J[1*], P. Jesu Jayarin[2]

[1]*Faculty of Information and Communication Engineering, Anna University, Chennai, INDIA.*
[2]*Department of Computer Science and Engineering, Jeppiaar Engineering College, Chennai, INDIA.*
nithisha.j@gmail.com, jjayarin@gmail.com

Abstract – Security is necessary today's fast computer world during the data communications in internet and cloud environment. The cloud security is becoming very challenging task today due to the presence of huge volume of cloud users. Even though, various cloud secured storage mechanisms are available and tried to fulfill the current requirement. However, not yet fulfill the cloud user's requirements in terms of security while storing and sharing the data in cloud. For this purpose, this work proposes a new secured storage and communication system for providing data security while storing the data in cloud database and sharing the data between the cloud users in cloud. This system consists of three different algorithms for performing prime number generation, digital signature creation for generating keys, encryption, decryption and authorization. In this paper, we propose a new technique to find a co-prime number which is used to generate keys in key generation process and also useful for performing encryption and decryption process. Moreover, a new key generation technique is also introduced for ECC and DSA using polynomial congruence for performing key generation process securely. In addition, a new Elliptic Curve and Polynomial Congruence based Encryption / Decryption algorithms for performing data encryption and decryption in the process of data storage and communication. Finally, the user authenticity is verified by the proposed digital signature algorithm in this work. The experiments have been conducted for evaluating the proposed secured storage and communication system and proved as better than others in terms of efficiency and security level.

Keywords – Elliptic Curves, Digital Signature Algorithm, Encryption, Decryption, Key Generation, Signature Generation, Signing and Verification.

* *Corresponding Author:* Nithisha J*, E-Mail:* nithisha.j@gmail.com

1. INTRODUCTION

The rapid growth of the networking technology in the past decade has improved the data exchange and data transmission. Due to the availability of various data such as text data, audio data, video data and image data in transmission, the drastic enhancement is required in data communication between the users and also required large volume of database for storing all these data as a cloud database. The cloud computing technology that facilitates the self-service to access the data from anywhere and anytime is unavoidable facility today's smart life (Garg et al., 2020). Moreover, it facilitates the remote storage and accessibility as important facilities. Here, the cloud storage is a basic necessity for supplying the required data to the concern cloud users. The various mechanisms have been developed for storing the cloud user's data efficiently with less expense (Ping et al., 2020). Generally, the data storage in cloud is not similar to the normal storage techniques and it needs huge storage space for storing the large volume of cloud user's data. Moreover, it must be able to allow the cloud users to access their data from different geographical area in the world (Sun et al., 2020).

Security is playing vital role in cloud environment due to the presence of huge volume of secret information and the large volume of authorized and unauthorized users as clients. Secured data communication in cloud is a very challenging issue in this fast internet and cloud era. The large volume of database is necessary to store the various kinds of cloud user's data with different variety of data in cloud. The cloud platform must be in the position to allow the users to store, share and access their data securely. The cloud users may be available in various countries in the world and they may store and access their data from various locations. In this scenario, the stored cloud data must be protected from the cloud users and anomalous users in the cloud environment. For this purpose, many secured routing protocols have been developed for transmitting the data between the users in the network by various researchers in the past. To provide the data security, the cryptographic algorithms are playing major role in the cloud. The data security and secured communication are necessary in the cloud environment due to the availability of different organizational users and their clients.

The administrator of the cloud database allows the cloud users to perform various roles and responsibilities on data accessibility and also permit to share their data from anywhere. The

conventional methodologies are applied in the past for protecting the cloud user's data with authentication. The various methodologies are trying to resolve the security problems such as privacy preservation, user's authentication, etc. by applying encryption and authorization techniques for restricting the data accessibility. Moreover, some of the researchers are concentrating over the cost efficiency, key generation and distribution time and the overall time complexity in data transmission. Majority works are concentrated to address the single owner scenarios that comes with high dependency. Recently, many works introduced for fulfilling the multi-owner issues as well and proved as better in cloud.

The data integrity is important today for activating the public audit service for the stored cloud data in the cloud database. The cloud users are authorized by a third-party auditor for performing auditing process on outsourced data when it is necessary. Generally, the cloud users are not performing any auditing process and it also requires a TPA for accomplishing the auditing task for the cloud users to ensure the cloud users data is appropriate (Shen et al., 2018). Moreover, the TPA is helpful for the CSP in terms of enhancing the cloud services in cloud (Li et al., 2020). Finally, the public auditing process is playing a significant function in emerging method as cloud user's requirement that means to evaluate the risks and earn confidence in the cloud.

The encryption, decryption and key generation techniques are useful for providing data security, data integrity, authentication and key generation processes. The standard algorithms such as AES, DES, RSA, ECC are applied for performing encryption process, decryption process and key generation process efficiently. Many cryptographic algorithms are used and also modified by various researchers for enhancing the performance in terms of security level and efficiency. Here, the encryption process is converting the plain text into ciphertext by applying a specific technique. The decryption process is converting the ciphertext into the plain text by applying a specific technique. The same encryption and decryption techniques are applied for generating the keys. Moreover, the Digital Signature Algorithm (DSA) is useful for validating the user authorization by performing the signing process and verification process. The DSA verifies the cloud user's authenticity and confirming the cloud user's authorization and allow the users to access the data.

The major contribution of this paper are as follows:

i) To propose a new prime number generation technique for generating prime numbers that are useful for generating the keys to perform the authentication process.

ii) To develop a new key generation technique for ECC for performing effective key generation process,

iii) To introduce a new ECC and Polynomial Congruence based Encryption / Decryption Algorithm (EPCEDA) for performing encryption and decryption processes. Here, the double encryption and double decryption are performed by using ECC and Polynomial congruence.

iv) To propose a new Digital Signature Algorithm (DSA) for ensuring the cloud users authentication by performing signature creation, signing and verification processes.

The reminder of the paper is organized as below: The existing relevant works have been discussed by highlighting the contributions. Merits and demerits in section 2 as literature survey. The working flow of the proposed model is explained through an architecture by showing all the necessary works and the relevant components in section 3. The graphical form of the working flow is demonstrated with necessary steps and background in section 4. Section 5 demonstrates the performance of the proposed secured storage and communication system with comparative analysis graphs. Section 5 provides the conclusion along with future works can be done further.

2. LITERATURE SURVEY

Many works have been done by the various researchers in this direction in the past. Among them, Elumalaivasan et al (2016) developed a new trust aware attribute encryption technique that considers the cipher text policies for retrieving the data with less time complexity. Their technique is helpful to improve the data security in networks while exchanging the data between the nodes of the network. Kendrekar and Chavan (2016) developed a novel key-based cryptosystem that performs decryption key generation method for decrypting the keys and also performs the decryption process on ciphertext while storing the data into the cloud database. In addition, they also discussed about the file modification in cloud. Potey et al (2016) focuses on providing the data confidentiality greatly for the data stored in the cloud. Generally, the homomorphic encryption

methods are useful for performing computational process on encrypted data with high computational cost. For this purpose, they have proposed a new homomorphic encryption method to perform encryption process efficiently by applying ECC method. Moreover, they have reduced the key size and also perform the less size cipher text.

Alrawais et al (2017) designed a new key exchange algorithm that incorporates the ciphertext policy aware ABE for performing secure data communication between the cloud users. They have combined two new techniques such as DSA and CP-ABE for performing the verification, confidentiality and authenticity. Finally, their model is proved as better than others in terms of feasibility. Nesrine et al (2017) conducted an extensive review about the cryptographic methodologies and also explored the research directions and the new methodologies for addressing the issues over the outsourced data protection in cloud.

Li et al (2017) proposed a new security based distributed storage mechanism that is useful for performing data distribution processes. They have evaluated their mechanism along with other methods and proved as efficient and secured. Subbulakshmi et al (2017) developed a new cloud aware POS mechanism to perform the shopping through online securely with the help of RFID. They have applied encryption and decryption processes to safeguard the online transactions. Mudepalli et al (2017) proposed a novel ciphertext retrieval method for retrieving the necessary data from huge volume of data. First, they have created index values for the data by applying the stemming operation and uses the blowfish method to perform the encryption process on data. Next, a new public key encryption aware ECC is also applied to generate keys that are useful for authenticating the cloud user's data accesses. Finally, the plaintext is retrieved by using blowfish method from the source data with low computational time and cost.

Thangapandiyan et al (2018) developed a modified ECC method for providing privacy preservation on sensitive cloud data. The modified ECC is applied for performing encryption and decryption processes whenever the users required their stored data in cloud after performing the verification process done by the admin. They have generated the private keys to decrypt the data with high encapsulation. Finally, their method proved as better than the existing conventional methods in terms of data security. Mehmood et al (2018) developed a healthcare system that contains a data privacy and anonymity for protecting the secret information from unauthorized

users. The proposed authentication method applied group signature technique that is developed using ECC for ensuring the data anonymity and also used an onion router for providing the data privacy in the network. Finally, their system proved as a secured one and also protects the data from attacks.

Vinod et al (2019) proposed a new protocol for ensuring the data security from the man-in-the-middle attack replay attack confidentiality authentication and session key security. They have compared their protocol with others for managing the efficiency in terms of less cost and time. Chen et al (2019) designed a new protocol for performing secure data transmission between the nodes in the network with good anonymity and scalability. Finally, it proved that as an efficient and scalable model than other models. Prabhu and Ganapathy (2019) developed a novel data storage method that uses the standard CRT to store the data securely in cloud database. Moreover, a new group key management method using CRT for retrieving the data from cloud. Their data storage method incorporates two encryption techniques with the application of two new formulas to perform two levels encryption process. Their method is evaluated by conducting various experiments and also proved as better than other works in terms of data security.

Yang et al (2020) developed a new privacy-preserving system for many cloud users with authorization. They have introduced a new authentication method that is able to work in between cloud service provider and third party auditor for protecting the data from DoS attacks. Their model avoids the certificate less verification which is ensured that the method is not involved the certification management process and proved as efficient method. Atiewi et al (2020) developed a cloud aware IoT environment with the incorporation of authentication process and a lightweight cryptographic encryption methodology for protecting the cloud data. The application of authentication process for accessing the cloud data through third party auditor that has three levels of authentications such as read, download and download from hybrid cloud. Finally, they have proved that their method is better than other methods in terms of efficiency and security.

Sheji et al (2020) developed a method which is efficient and publicly verifiable in cloud that provide security to the data while transferring the data from one user to another one user. They have introduced a cryptosystem that works based on bilinear key aggregation process by applying key aware homomorphic authenticated privacy preservation method to ensure the data security in

data transmission. Moreover, their method is achieved key auditing process successfully for reducing the computational complexity and also proved as an efficient than other methods. Tran et al (2020) developed a new authentication method for providing secure control from servers to devices when enables the secure communication in between the cloud users in cloud. Their method is developed by applying ECC for consuming the resources. Finally, they have proved as better than the existing methods.

Mohana and Vidhya (2020) proposed a new authentication scheme which incorporates the suppressed k-anonymity multi-factor authentication method aware Schmidt-Samoa cryptography that comprises the key registration, authentication and data accessibility for preserving the client's data. Finally, their scheme is also performed the authentication process and also avoid the insecure data communication in between the clients in the cloud. At the end, their scheme proved as better than other schemes in terms of security level. Khan et al (2020) constructed a new framework for accessing the e-healthcare data through mobile devices. It starts with the authentication process that incorporates SHA-512 method for ensuring the authentication process while transmitting the data in cloud. It is also ensured the data integrity by applying the two types of encryption processes by using Ceaser Cipher and Improved ECC. In the improved ECC, a new secret key is generated for enhancing the security with less time complexity than the standard encryption methods. Kavin and Ganapathy (2020) developed a new Elliptic Curve and Diffie-Hellman aware method to secure the data securely in cloud. The existing DH method is applied two times along with ECC to store the data securely in cloud. The performance of the system is evaluated through experimental results for the various inputs and also proved as better than the standard ECC and DH methods.

Pradeep et al (2021) developed a novel cryptosystem that incorporates the ECC and the Matrix translation to perform secure data communication through a routing method and also ensured the energy efficiency. They have performed the key generation process, encryption process, decryption process and the cluster aware routing process. Moreover, they have introduced prime number generation table, string position aware ASCII value contained reference table for performing encryption and decryption processes effectively. Finally, their cryptosystem enhances the data security along with the overall network performance in terms of packet delivery ratio. Kavin and Ganapathy (2021) developed an Enhanced DSA to verify the data integrity while storing the data in cloud. Here, the elliptic curves are generated for enhancing the performance. The

generated curve points are applied as a public key that is helpful for performing the signing process and the verification process. Moreover, two new formulas have been introduced to perform signing process and the verification process and also useful for comparing the document originality checking process. At the end, the efficiency of their model is proved in terms of key generation, signing and verification times through various experimental results. Pavani et al (2021) addresses the various security issues and also developed a novel secure cloud storage method according to the game theory-based polling user access or game theory based getting user access for protecting the data. Sowjanya et al (2021) developed an enhanced version of lightweight ECC aware authentication method for performing authentication process successfully. Moreover, they have evaluated the security formally and informally for proving the strength of their method in terms of security.

3. SYSTEM ARCHITECTURE

The overall architecture of the proposed work is shown in figure 1 that contains eight major components such as cloud database, cloud user, decision manager, Cloud Service Provider (CSP), Third Party Auditor (TPA), Key generation Phase, Encryption / Decryption Phase and Digital Signature Algorithm (DSA) phase.

In this work, the cloud user will be authorized by the TPA and then allow to access the data according to the user's rights. This authorization process is also start with the key generation phase. The cloud database contains the huge volume of data that are stored by the various cloud users in the cloud. The cloud user is able to store and access their data through CSP. The CSP facilitates to the cloud users for storing and accessing their data through decision manager. The decision manager has control over the entire components of of this overall architecture. The decision manager analyzes the cloud users requests and permit them to access through TPA. The TPA is helpful for identifying the user genuineness by verifying their keys. The key generation phase contains three sub components such as prime number generation, DSA for key generation and ECC based key generation. The first component of this key generation phase is responsible to generate prime numbers that are helpful for generating the secret keys as public and private keys. The second component of this key generation phase is used to generate the keys by applying the DSA. Third component of this work is to generate keys by using Elliptic curve points that are

generated by ECC. This phase uses the proposed ECC based Key Generation Algorithm (ECKGA) for generating keys.

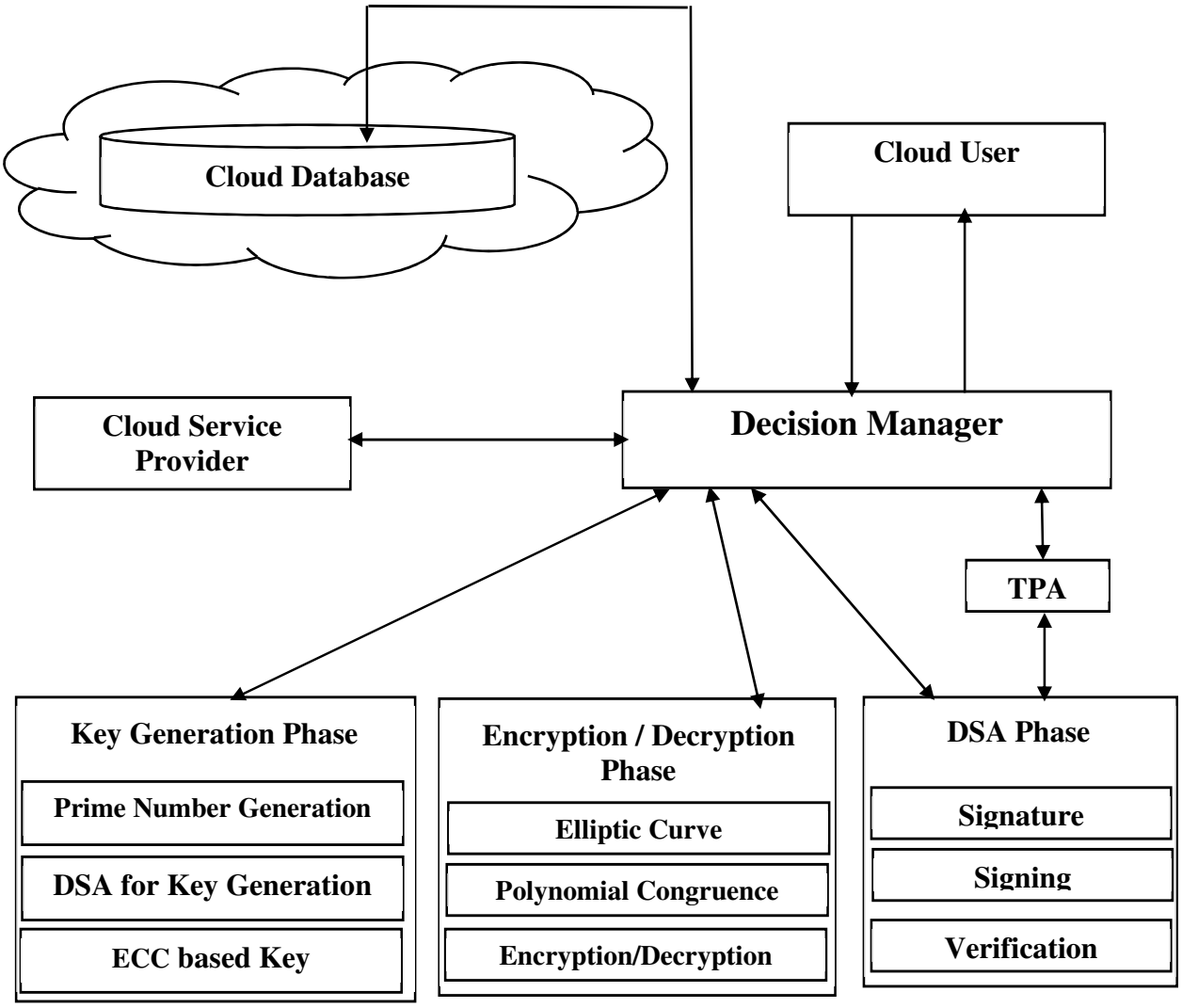

Figure 1. Secured Storage and Communication System

The encryption/decryption phase contains three major components such as elliptic curve points generation, polynomial congruence and Encryption / Decryption process. Here, the elliptic curve points are to be generated by using the ECC. Find the polynomial congruence and perform the encryption process and decryption processes. This phase applies the proposed ECC and Polynomial Congruence aware Encryption / Decryption algorithm (ECPCEDA) for performing encryption and decryption processes. The Digital Signature Algorithm (DSA) phase consists of three components such as signature creation, signing and verification for performing the signature

generation process, signing process and verification process effectively. This phase applies a newly proposed digital signature algorithm for authorizing the cloud users through performing three different tasks.

Generally, this system stored the cloud user's data in the cloud database in the form of ciphertext through CSP and decision manager. At the same time, the stored data can be accessed by the cloud users after involving the proper authentication process done by the TPA with the help of DSA phase. The decision manager will respond to the cloud users according to their requests and the data availability. The encrypted data (Cipher text) is stored in the cloud database. According to the cloud user's request, the decision manager gets the encrypted data from cloud database. Finally, the decision manager provides the requested data by decrypting the data from ciphertext to plaintext with the help of encryption / decryption phase through CSP.

4. PROPOSED WORK

This section describes in detail about the proposed secured storage mechanism that contains the proposed new Key Generation technique for ECC, key generation technique for DSA, ECC and Polynomial Congruence based Encryption/Decryption algorithm (ECPCEDA) for performing double encryption and decryption processes on cloud user's data to the cloud database securely. Moreover, it contains three sections such as Key Generation, Encryption/Decryption and Digital Signature. First, the background of ECC and Polynomial Congruence are discussed in this section.

4.1 Background

This sub section describes the background detail of Elliptic Curve Cryptography (ECC) and the Polynomial Congruence. First, the ECC is explained with necessary diagram and equations by highlighting the need and merits.

4.1.1 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) provides a suitable cryptographic technique for providing security on data communications in wireless sensor networks because of its key sizes and efficiency in the provision of security. Moreover, effective key management techniques that are

compatible with the calculations for cryptographic algorithms are necessary to meet the increasing speed and security requirements in current applications. Therefore, it is necessary to reduce the key size of the public key encryption protocols for fast key calculation and effective encryption. In addition, the key generation process should include the computation of additional functions to improve the communication security. Therefore, important functions in mathematical theory have been used in this research work to create the most secure keys enhance the security strength of Elliptic Curve Crypto system.

The "Elliiptic" is not equation is ellipse and the general framework of the curve is generated based on the formula is shown in equation (1).

$$y^2 = x^3 + ax + b \qquad (1)$$

Here, the variables 'a' and 'b' are representing the real numbers along with the values 2 and 1 respectively. Figure 2 shows the curve that is generated according to the equation (1). In general, the curve is used to generate keys by considering any one / two points randomly.

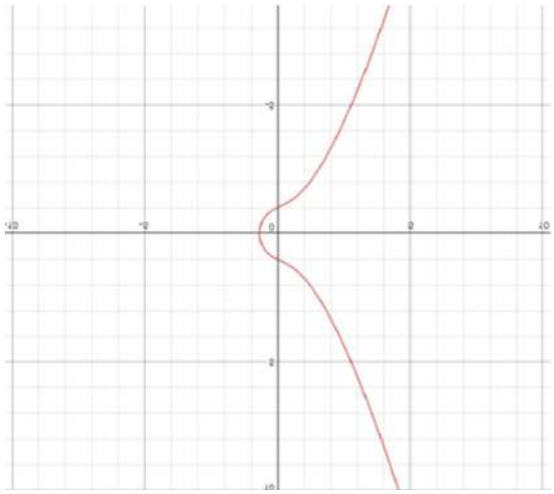

Figure 2. Elliptic curve

4.1.2 Polynomial Congruence

The polynomial congruence is defined as follows: Let assume that P(x) is the integral polynomial and these are to be expressed as given in equation (2)

$$P(x) \equiv 0 \ (mod\ n) \qquad (2)$$

And it is also called as polynomial congruence. Moreover, the linear congruence is also considered as polynomial congruence with the form given in equation (3)

$$a_0 + a_1 x \equiv 0 \ (mod\ n) \qquad (3)$$

where, 11 is the degree of the integral polynomial. In addition, this kind of congruence is encountered frequently as per the given structure in equation (4).

$$ax \equiv b \ (mod\ n) \qquad (4)$$

For example, let consider the polynomial f with coefficients and the congruence equation $f(x) \equiv 0 \ (mod\ n)$ is known as polynomial congruence. To resolve the following using polynomial congruence.

$$x^3 + 2 \equiv 0 \ (mod\ 9)$$

Let assume that x = 0, 1 and 2. First, consider 1 is the value of x. The modulo 9 is equivalent to 1 modulo 3.

4.2 Key Generation

The key generation is playing major role for performing encryption, decryption and authorization in cloud. First, this work needs two random prime numbers by using the prime number generation process that is shown in Algorithm 1. Generally, two prime numbers are to be chosen randomly for verifying the algorithm. This work chosen a prime number randomly. The chosen prime number will generate new prime number by applying new technique (nq+1). Then, chosen a hash value which is less than q-1 and greater than 1. Afterwards, the g value is generated by using the prime number p and hash value.

Algorithm 1: Prime Number Generation

INPUT: Random prime number q;

OUTPUT: Domain parameters (p, q, g);

Step 1: Choose a random large prime number q.
Step 2: Calculate the prime number p = nq + 1 where n (even number) = 2 to (q-1).
Step 3: Identify a hash value (h) using Hash () function and the value is to be $1 < h < q-1$.
Step 4: Compute the g value using the formula $g = h^n \bmod p$.

This algorithm generates a prime number randomly as q and find the biggest prime number. Finds the hash value for the input value and to find the g value by performing modulo operation for the hash value and the prime number. These three values p, q and g are used to generate the keys in ECC and DSA.

The steps of the key generation technique for digital signature algorithm are as follows:

Algorithm 2: Key Generation for DSA

INPUT: Domain parameters (p, q, g);

OUTPUT: signer's private key's e_1, e_2; signer's public key's d_1, d_2; a secure hash function Hash (h) with output of length |q|.

Step 1: Choose a random number e_1 within the range of |q|.
Step 2: Calculate d_1 from e_1 by using $d_1 = g^{e}_1 \bmod p$.
Step 3: Find the value of e_2 using $e_2 = e_1^{-1} \bmod q$.
Step 4: Compute the d_2 value using $d_2 = e_2^{-1} \bmod p$.

The digital signature algorithm based key generation considers the two prime numbers p and q along with g value as input. The output for the given input is the private keys such as e1 and e2, public keys such as d1 and d2. Finds the privates keys by applying the modulo operation on prime numbers and the private and public keys.

The Key Generation technique for ECC is explained with necessary steps in Algorithm 3.

Algorithm 3: Key Generation for ECC

INPUT: Domain parameters (p, q, g);

OUTPUT: Elliptic Curve $E_p(a,b)$; Private key's d_A, d_B; Public key's P_A, P_B; x_1, x_2;

Step 1: Choose 'a' is the entry position of the user and the value of 'b = 0'.

Step 2: Compute ECC equation $E_p(a,b)$.

Step 3: Generate the points on the Elliptic Curve $y^2 = x^3 + ax + b \bmod p$.

Step 4: Choose the Generator G and random points d_A, d_B as private keys from the generated points.

Step 5: Compute Public Keys $P_A = G \times d_A$ and $P_B = G \times d_B$.

Step 6: Let's consider the polynomial congruence on Elliptic Curve $f(x_1) = x_1^3 + ax_1 + b$ and find the x_1 value with the condition of $f(x_1) \equiv 0 \pmod p$.

Step 7: Find $f'(x_2) = 3x_2^2 + a$ and find the x_2 value with the condition of $f'(x_2) \equiv 0 \pmod p$.

The proposed ECKGA provides the elliptic curves, private keys and public keys as output for the given input such as p, q and g. Here, first find the starting position of the cloud user and the value is considered as 0. Find the ECC equation for the two positions (a, b). Then, generates points by using the elliptic curve formula and also generates the random points (d_A, d_B) as private keys. Finally, it finds the public keys.

4.2 Digital Signature Algorithm

This subsection explained in detail about the proposed digital signature algorithm that is helpful for verifying the cloud user's authorization process. The signature generation and verification processes are discussed in this section with the proposed DSA. First, the signature creation algorithm is explained with necessary steps.

A. Signature Creation

The subsection is explained about the signature creation process with necessary steps. The signature creation is important part in the authentication process. By using this signature only, the

cloud users can be authorized for storing and accessing their data in cloud environment. The steps of the signature creation algorithm are as below:

Algorithm 4: Signature Creation Algorithm

INPUT: Domain parameters (p, q, g); private key e_1; public key d_2; a secure hash function Hash(h) with output of length |q|.

OUTPUT: Signature (r,s).

Step 1: Choose a random 'i' in the range [1,q−1].
Step 2: Find the y value using the formula $y = g^i \bmod p$
Step 3: Compute the r value using $r = y \bmod q$. If r = 0 then go to step 1.
Step 4: Find the i^{-1} by applying modulo operation on q.
Step 5: Find the hash value h using Hash(M) function that is to be an integer in the range $0 \leq h < q$.
Step 6: Find the t value using the formula $t = i^{-1}(h+e_1r) \bmod q$. If t=0 then go to step 1.
Step 7: Calculate $s = td_2^i \bmod p$.
Step 8: Return (r, s).

The signature creation process is done with eight steps. It starts with selecting the range and calculates the values of y, r, h, t and s by applying the modulo operation. Finally, it returns the signature as two variables r and s. First, choose a random number "I" within the range of 1 and q-1. Calculate the y value by using the newly generated prime number p and the value g to compute the r value which is used to verify the signature. If the r value is 0 which is obtained from y mod q then choose another "i" value. Next, the t value needs to be calculated. For this purpose, inverse of i mod q is to be calculated and applied along with hash value and private key value. If t=0 then repeat the earlier steps. Then, the s is to be calculated by using the values of d, t and p. Finally, it returns the signature.

B. Signature Verification

This subsection explains in detail about the signature verification process by applying the proposed signature verification technique. The steps of the proposed signature verification technique are as follows:

Algorithm 5: Signature Verification

INPUT: Domain parameters (p, q, g); private key e_2; public key d_1; a secure hash function Hash(h) with output of length |q|; signature (r, s) to be verified.

OUTPUT: "Accept" or "Reject".

Step 1: Verify that r and s are in the range [1, q−1]. If not then return "Reject" and stop.
Step 2: Calculate the z value using $z = e_2^i \bmod p$ for finding the x value.
Step 3: Find the x value using $x = z \,.\, s \bmod p$ for finding the value of w.
Step 4: Find the value of w using the formula $w = x^{-1} \bmod q$ for knowing the value of u_1.
Step 5: Find the hash value (h) using the Hash(M) function that is to be an integer and in the range $1 < h < q$.
Step 6: Calculate the value of u_1 using $u_1 = hw \bmod q$ for finding y value.
Step 7: Find the u_2 value by using the formula $u_2 = rw \bmod q$ for knowing the y value.
Step 8: Calculate the y value using the formula $y = g^{u1} d_1^{u2} \bmod p$ to find the v value.
Step 9: Calculate the v value by applying the formula $v = y \bmod q$ to perform the verification.
Step 10: If v = r then return "Accept" otherwise return "Reject".

The signature verification process is done by applying the necessary steps of the signature verification algorithm which is a part of the digital signature algorithm. First, it verifies the signature range. If it is equal range then accept it for further processing or it will be rejected. Next, find the z,x and w values by applying modulo operation and the h value is to be calculated by using the hash function and it will be checked whether it is less than the q value and greater than 1. Then, finds the u1, u2, y and v values by applying modulo operations. Finally, it verifies the value r is equivalent to v or not. If these values are equal then it is acceptable and the cloud user is to be allowed to access the data or the users request is to be rejected.

4.3 Encryption / Decryption

The data encryption and decryption processes are explained in this sub section in detail. The cloud data encryption is done by using the proposed ECC and Polynomial based Encryption algorithm. First, the cloud user's data is to be encrypted as ciphertext from plain text by using the following steps:

Algorithm 6: ECC and Polynomial Congruence aware Encryption

INPUT: Domain parameter p; Polynomial equation $f(x_1)$; Generated Points on the Elliptic Curve; Private key's d_A; Public key's P_A, P_B; Polynomial Congruence; Plain Text 'm'; x_1;

OUTPUT: Encrypted Text;

Step 1: Choose random point P from the generated points.
Step 2: Find the Q value using the formula $Q = d_A \times P$
Step 3: Calculate the value of C_1 using $C_1 = P_A \times P$
Step 4: Compute $M_e = m + f(x_1)$ using Polynomial Congruence to perform second level encryption.
Step 5: Find the value of C_2 using $C_2 = M_e + (P_B \times Q)$ and perform encryption process.

The encryption process considers the polynomial equation, Elliptic curve points, private keys, public keys, polynomial congruence and the plain text as input and it produce encrypted text as output. Here, the P is the random point which is one of the ECC point. Then, the P is used to calculate the value Q and C1 that are the additional parameters in encrypted text. These values are useful for performing decryption process. Then, apply the polynomial congruence technique on encrypted message to perform first level encryption. Finally, the second level encryption is to be done for the output of first level encryption text.

The encrypted content is decrypted by using the proposed ECC and Polynomial Congruence based decryption algorithm. The steps of the proposed algorithm are as follows:

Algorithm 7: ECC and Polynomial Congruence aware Decryption

INPUT: Domain parameter p; Polynomial equation f'(x_2); Encrypted Text; Private key's d_B; Polynomial Congruence; x_2;

OUTPUT: Encrypted Text;

Step 1: Compute $M_d = C_2 - (d_B \times C_1)$
Step 2: Apply the polynomial congruence to decrypt the Original Text 'm' = M_d + f'(x_2) (mod p)

The encrypted text (ciphertext) is converted into plain text by considering the polynomial equation, encrypted text, private keys and congruence as input and it produce a suitable output in the form of plaintext. Here, the first level decryption is to be done using ECC and the second level decryption is to be done by applying polynomial congruence.

4.4 Mathematical Proof

The working flow of the proposed secured storage and communication system is demonstrated in this section by applying input values for all the algorithms. First, the key generation process is explained based on the algorithm steps.

4.4.1 Key Generation

In this work, the key generation is important to perform encryption, decryption, digital signature creation and verification processes.

A. Prime Number Generation:

INPUT: Random prime number q;

OUTPUT: Domain parameters (p, q, g);

1. Choose a random prime number q = 29.
2. Compute prime number p = nq + 1 where n (even number) = 2 to (q-1).

Choice 1: $n = 2$

$p = (2 \times 29) + 1 = 58 + 1 = 59$ (It is Prime number)

$p = 59$.

3. Choose h Hash () with $1 < h < q-1$.

   $h = 14$

4. Compute $g = h^n \bmod p$.

   $g = 14^2 \bmod 59 = 19$

End of this prime number generation technique, three values such as p, h and g are generated as 59, 14 and 19. Then, the values of p, q and g are passed as input to the key generation technique of DSA.

B. Key Generation for DSA

The randomly given prime number is 29 and newly generated prime number is 59, and another one value 19 are considered as input for the Key generation for DSA.

INPUT: Domain parameters (p = 59, q = 29, g = 19);

OUTPUT: Signer's private key's e_1, e_2; signer's public key's d_1, d_2;

1. Choose a random number e_1 within the range of $|q|$.

   $e_1 = 18$

2. Compute d_1 from e_1, $d_1 = g^{e}{}_1 \bmod p$.

   $d_1 = 19^{18} \bmod 59 = 26$

3. Compute e_2, $e_2 = e_1^{-1} \bmod q$.

   $e_2 = 18^{-1} \bmod 29 = 21$

4. Compute d_2, $d_2 = e_2^{-1} \bmod p$.

   $d_2 = 21^{-1} \bmod 59 = 45$

The private and public keys are to be generated by using the prime numbers and other number as well. Here, the value 18 is chosen as random number and also generates the values of d1, e2 and d2 that are useful for creating DSA.

C. Key Generation for ECC

The values of p, q and g are considered in this work for generating keys for ECC.

INPUT: Domain parameters (p = 59, q = 29, g = 19);

OUTPUT: Elliptic Curve $E_p(a,b)$; Private key's d_A, d_B; Public key's P_A, P_B; x_1, x_2;

1. Choose 'a = 18' is the entry position of the user and the value of 'b = 0'.
2. Compute ECC equation $E_{59}(18,0)$.

   $y^2 = x^3 + 18x \bmod 59$
3. Generate the points on the Elliptic Curve $y^2 = x^3 + 18x \bmod 59$.

   (0,0) (10,0) (49,0) (1,14) (3,9) (6,18) (6,41) (8,19) (8,40) (13,22) (14,20) (15,20) (14,39) (15,39) (17,26) (18,16) (18,43) (19,11) (19,48) (20,10) (21,9) (21,50) (25,26) (25,33) (26,7) (28,6) (28,53) (30,20) (30,39) (32,3) (35,9) (35,50) (36,24) (36,35) (37,15) (43,10) (43,49) (47,11) (47,48) (48,8) (48,51) (50,17) (50,42) (52,11) (52,48) (54,27) (54,32) (55,10) (55,49) (57,29) (57,30).
4. Choose the Generator G and random points d_A, d_B as private keys from the generated points.

   G = (8,19), d_A = (19,11), d_B = (25,33)
5. Compute Public Keys $P_A = G \times d_A$ and $P_B = G \times d_B$.

   $P_A = G \times d_A$ = (152,209)

   $P_B = G \times d_B$ = (200,627)
6. Let's take $f(x_1) = x_1^3 + ax_1 + b$ and find the x_1 value with the condition of $f(x_1) \equiv 0 \pmod p$.

   $f(x_1) = x_1^3 + 18x_1 \equiv 0 \pmod{59}$

   If $x_1 = 1$, then $(1)^3 + 18(1) = 19 \equiv 0 \pmod{59}$ [Condition not satisfied]

   If $x_1 = 2$, then $(2)^3 + 18(2) = 44 \equiv 0 \pmod{59}$ [Condition not satisfied]

   .

   .

   .

   If $x_1 = 10$, then $(10)^3 + 18(10) = 1180 \equiv 0 \pmod{59}$ [Condition satisfied]

   Therefore, $x_1 = 10$.
7. Find $f'(x_2) = 3x_2^2 + a$ and find the x_2 value with the condition of $f'(x_2) \equiv 0 \pmod p$.

f'(x_2) = $3x_2^2 + a \equiv 0 \pmod{59}$

If $x_2 = 1$, then $3(1)^2 + 18 = 21 \equiv 0 \pmod{59}$ [Condition not satisfied]

If $x_2 = 2$, then $3(2)^2 + 18 = 30 \equiv 0 \pmod{59}$ [Condition not satisfied]

.

.

.

If $x_2 = 17$, then $3(17)^2 + 18 = 885 \equiv 0 \pmod{59}$ [Condition satisfied]

Therefore, $x_2 = 17$

4.4.2 Digital Signature

The proposed digital signature algorithm is explained with necessary steps and contents in this work. Generally, the digital signature algorithm consists of three phases such as digital signature creation, signing and verification. First, the signature creation/generation is explained.

A. Signature Creation

INPUT: Domain parameters (p = 59, q = 29, g = 19); private key $e_1 = 18$; public key $d_2 = 45$; a secure hash function Hash(h) = 14 with output of length |q|.

OUTPUT: Signature (r,s).

1. Choose a random 'i = 8' in the range [1,q−1].
2. Compute $y = g^i \bmod p$
   $y = 19^8 \bmod 59 = 41$
3. Compute r = y mod q. If r = 0 then go to step 1.
   r = 41 mod 29 = 12
4. Compute $i^{-1} \bmod q$.
   $i^{-1} \bmod q = 8^{-1}$ 06d 29 = 11
5. Compute h = Hash (M) where $0 \leq h < q$.
   h = 14
6. Compute $t = i^{-1}(h+e_1 r) \bmod q$. If t=0 then go to step 1.

t = 11(14+(18x12)) mod 29

t = 2530 mod 29

t = 7

7. Compute $s = td_2^i \bmod p$.

   $s = 7 \times 45^8 \bmod 59$

   s = 48

8. Return (r, s) = (12, 48)

The digital signature (12,48) is created for the given input values (59,29 and 19) along with additional values (18, 45, 14).

B. Signature Verification

INPUT: Domain parameters (p = 59, q = 29, g = 19); random number i = 8; private key $e_2 = 21$; public key $d_1 = 26$; a secure hash function Hash(h) = 14 with output of length |q|; signature (r, s) = (12, 48) to be verified.

OUTPUT: "Accept" or "Reject".

1. Verify that r is in the range [1, q−1]. If not then return "Reject" and stop.

   r = 12 is in the range $1 < r = 12 < q-1$.

2. Compute $z = e_2^i \bmod p$.

   $z = 21^8 \bmod 59 = 53$

3. Compute x = z . s mod p

   $x = (53 \times 48) \bmod 59 = 7$

4. Compute $w = x^{-1} \bmod q$.

   $w = 7^{-1} \bmod 29 = 25$

5. Compute h = Hash(M) = 14 in the range $1 < h < q$.

6. Compute $u_1 = hw \bmod q$

   $u_1 = (14 \times 25) \bmod 29 = 2$

7. Compute $u_2 = rw \bmod q$.

   $u_2 = (12 \times 25) \bmod 29 = 10$

8. Compute $y = g^{u1}d_1^{u2} \bmod p$

   $y = 19^2 \times 26^{10} \bmod 59 = 41$

9. Compute $v = y \bmod q$.

   $v = 41 \bmod 29 = 12$

   $v = 12$

10. If v = r then return "Accept" otherwise return "Reject".

    v = 12 = r. So, it is accepted.

4.4.3 Encryption / Decryption

A. Encryption

INPUT: Domain parameter $p = 5$; Generated Points on the Elliptic Curve; Private key's $d_A = (19,11)$; Public key's $P_A = (152,209)$, $P_B = (200,627)$; Polynomial Congruence; Plain Text 'm = 34'; $x_1 = 10$;

OUTPUT: Encrypted Text;

1. Choose random point P = (15,20) from the generated points.
2. Compute $Q = d_A \times P$

   $Q = d_A \times P = (19,11) \times (15,20) = (285,220)$

   $Q = (285,220)$

3. Compute $C_1 = P_A \times P$

   $C_1 = (152,209) \times (15,20) = (2280,4180)$

   $C_1 = (2280,4180)$

4. Compute $M_e = m + f(x_1)$

   $M_e = 34 + x_1^3 + 18x_1$

   $= 34 + 10^3 + (18 \times 10)$

   $= 34 + 1000 + 180$

   $M_e = 1214$

5. Compute $C_2 = M_e + (P_B \times Q)$

   $C_2 = 1214 + [(200,627) \times (285,220)]$

C_2 = (58214,139154)

B. Decryption

INPUT: Encrypted Text C_1 = (2280,4180), C_2 = (58214,139154); Domain parameter p = 59; Private key's d_B = (25,33); Polynomial Congruence; x_2 = 17;

OUTPUT: Decrypted Text;

1. Compute $M_d = C_2 - (d_B \times C_1)$

   $M_d = C_2 - (d_B \times C_1)$

   $= (58214,139154) - [(25,33) \times (2280,4180)]$

   $M_d = 1214$

2. Decrypt the Original Text 'm' = $M_d + f'(x_2) \pmod p$

   $m = 1214 + 3x_2^2 + 18 \pmod{59}$

   $= 1214 + 3(17)^2 + 18 \pmod{59}$

   $= 1214 + 867 + 18 \pmod{59}$

   $= 2099 \pmod{59}$

   $m = 34$

Decrypted Original Text 'm' = 34.

In this work, the encryption and decryption process are done double times by using ECC and the polynomial congruence.

5. RESULTS AND DISCUSSION

The proposed secured storage and communication system has been implemented by using Java programming and deployed in Amazon web service. The proposed system is evaluated by conducting various experiments to prove the data security, data integrity, cloud user's authentication process and the security level in cloud while storing and retrieving the data by the cloud users. This system is considered the key generation time, encryption time, decryption time, key size and file size. The various number of experiments have been done for proving the proposed

system is efficient than other models in terms of time taken for performing key generation, encryption, decryption and file analysis.

First, the key generation time is considered and compared with other standard technique. Figure 3 shows the key generation time analysis between the standard RSA, Prabhu et al (2021) and the proposed model. Here, the key generation time is considered as milli seconds. Moreover, this time analysis is conducted by considering the 512 bits size of key for the different sizes of files. Here, five different experiments have been considered for evaluating the performance.

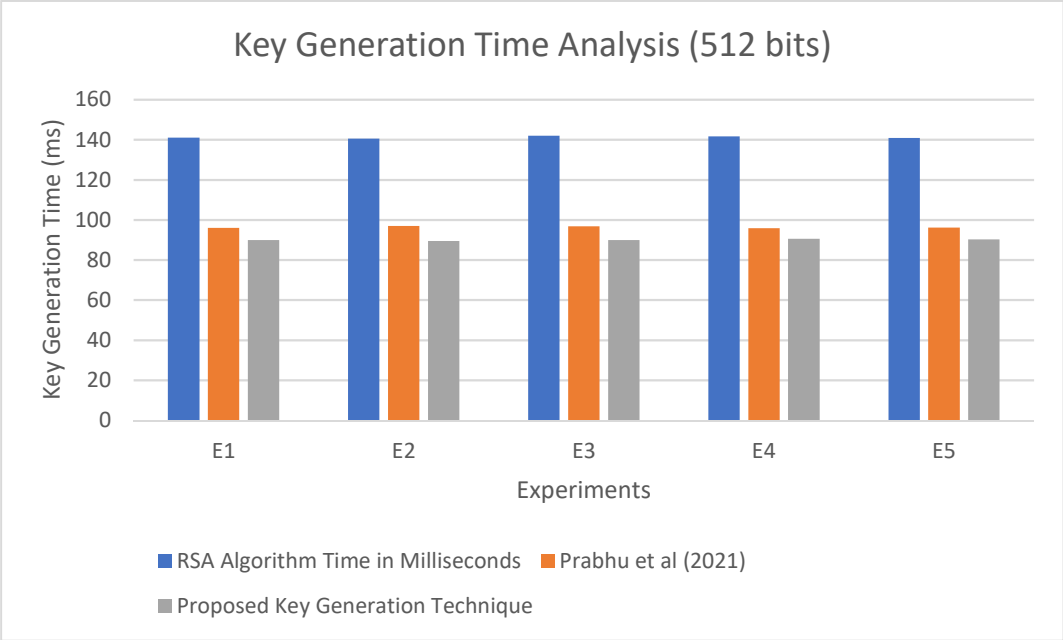

Figure 3. Key Generation Time Analysis for 512 bits size keys

From figure 3, the performance of the proposed key generation technique is better when compared to the existing techniques that uses RSA and ECC for generating keys. The betterment of the proposed key generation technique is the introduction of new technique incorporated for generating keys along with ECC.

Figure 4 shows the key generation time analysis between the standard RSA, Prabhu et al (2021) and the proposed model. Here, the key generation time is considered as milli seconds. Moreover, this time analysis is conducted five different experiments by considering the 1024 bits size of key

for the different sizes of files. Here, five different experiments have been considered for evaluating the performance.

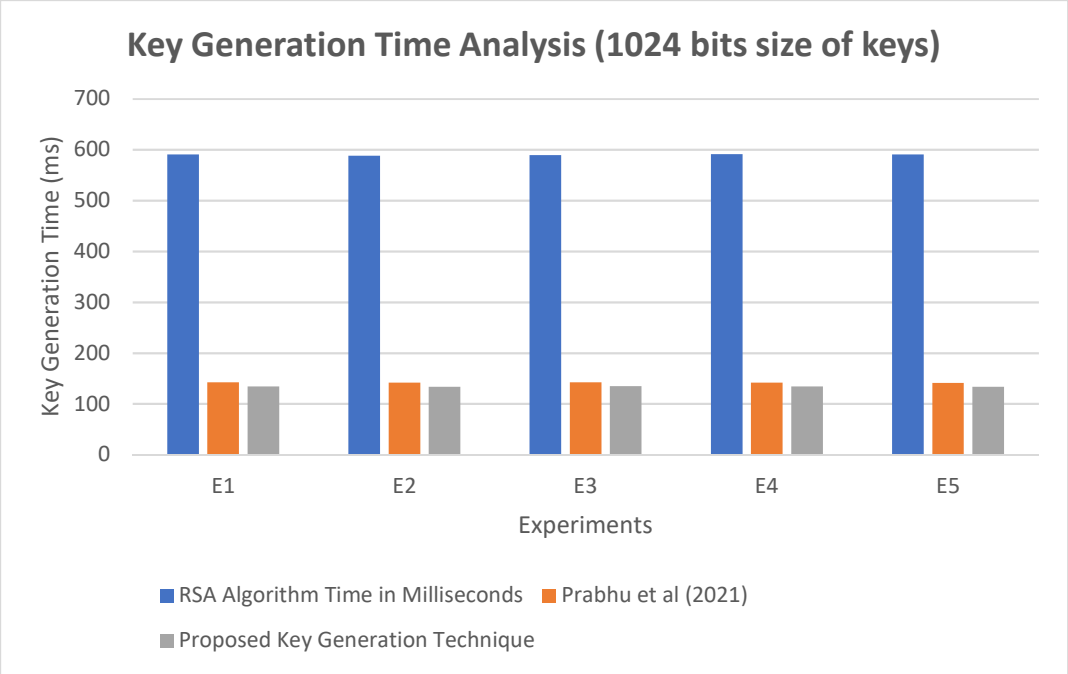

Figure 4. Key Generation Time Analysis for the 1024 bits size of key

From figure 4, the performance of the proposed key generation technique is better when compared to the existing techniques that uses RSA and ECC for generating keys. The betterment of the proposed key generation technique is the introduction of new technique incorporated for generating keys along with ECC.

Figure 5a to 5d demonstrate the time analysis of key generation, encryption, decryption and file size analysis for the original plain text contained input file and the encrypted file that contains the plaintext in the encrypted version. Here, figure 5a demonstrates that the key generation time analysis for the standard AES, technique proposed by Prabhu et al (2021) and the proposed model. Figure 5b demonstrates that the encryption time analysis for the standard AES, prabhu et al (2021) and the newly proposed model. Figure 5c demonstrates that the decryption time analysis for the standard AES, prabhu et al (2021) and the newly proposed system. Figure 5d demonstrates that

the file size analysis for the standard AES, Prabhu et al (2021) and the newly proposed secured storage and communication system.

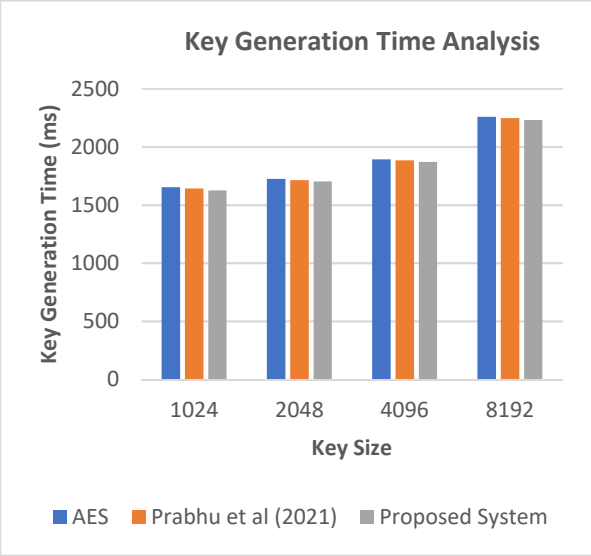

Figure 5a. Key Generation Time Analysis

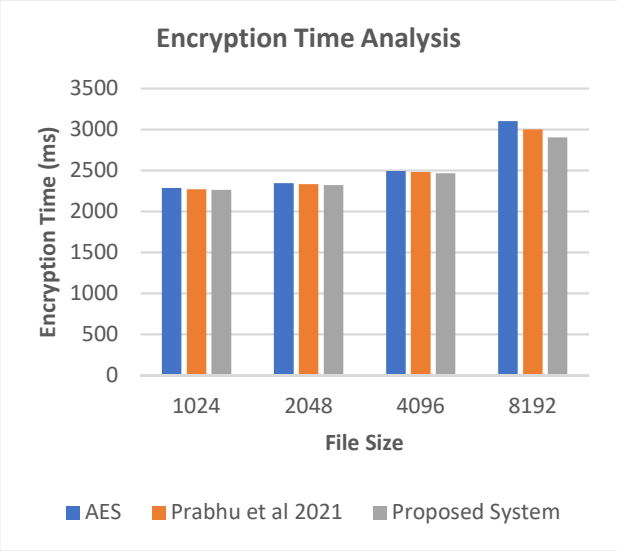

Figure 5b. Encryption Time Analysis

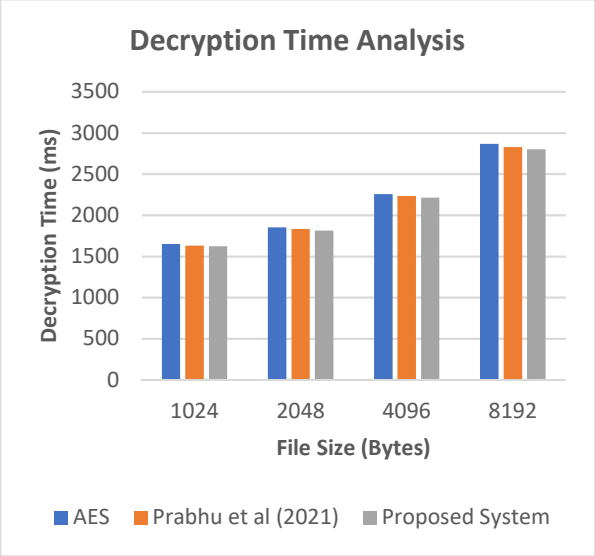

Figure 5c. Decryption Time Analysis

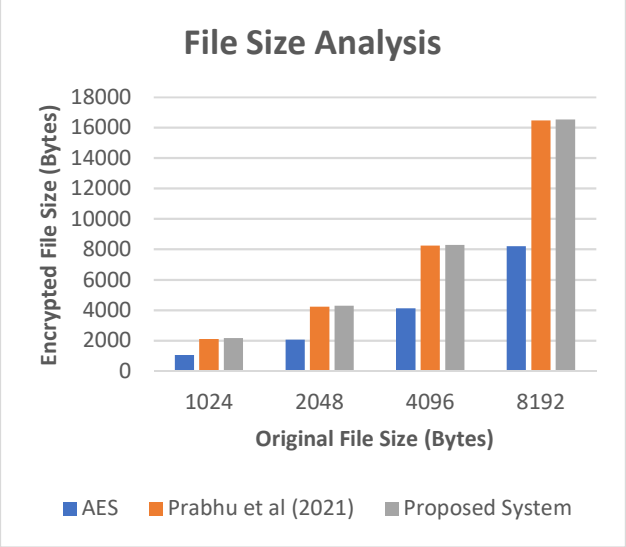

Figure 5.d. File Size Analysis

From figure 5a, it is proved that the proposed system efficiency which is better the standard AES and the technique proposed by Prabhu et al (2021) in terms of key generation time. The proposed

secured storage and communication system consume less time for generating keys when it is compared to the time taken by the standard AES and another one technique developed by Prabhu et al (2021). The reason for the enhancement is the application of new technique on key generation process along with ECC. From figure 5b, it can be seen that the proposed secured storage and communication system consumed less time to encrypt the plain text than the standard AES and the work done by Prabhu et al (2021). This is due to the fact that the application of new technique on key generation and also uses the polynomial congruence. From figure 5c, it is seen that the effectiveness of the proposed system in terms of taking minimum time to decrypt the cloud user document when it is compared to the time taken by AES and the Prabhu et al (2021) for the various files with different sizes. This is due to the fact that the application of ECC, double encryption and decryption through Polynomial Congruence. From figure 5d, it is proved that the performance of the proposed system is better than the standard AES and the technique proposed by Prabhu et al (2021). The reason for the improvement is the application of double encryption and double decryption process by using ECC and Polynomial Congruence and also applied new technique for key generation.

Figure 6 to 9 demonstrate the time analysis of the key generation process, encryption process, decryption process and the file size analysis between the plaintext contained original file and the ciphertext contained encrypted file. Here, figure 6 demonstrates that the key generation time analysis by considering the standard DES, the work done by Prabhu et al (2021) and the proposed secured storage and communication system.

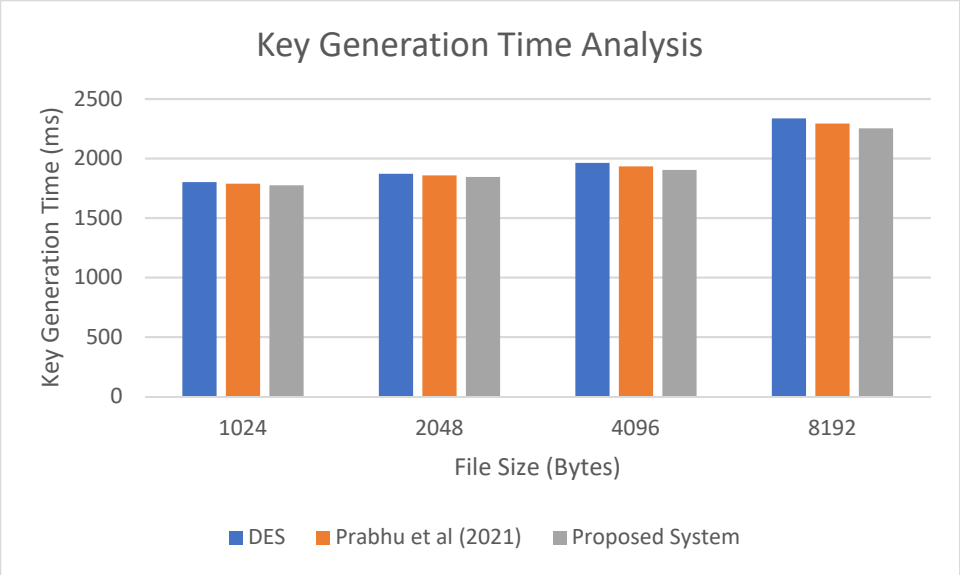

Figure 6. Key Generation Time Analysis considering different sizes of files

From figure 6, it is proved that the efficiency of the proposed system is better when it is compared with the standard DES and the work done by Prabhu et al (2021) in terms of time taken for performing key generation process. This is due to the fact that the use of polynomial congruence, EECC and the new key generation technique.

Figure 7 demonstrates that the encryption time analysis by considering the standard DES, Prabhu et al (2021) and the proposed system. Here, the different sizes of files were considered to find the encryption time for performing comparative analysis.

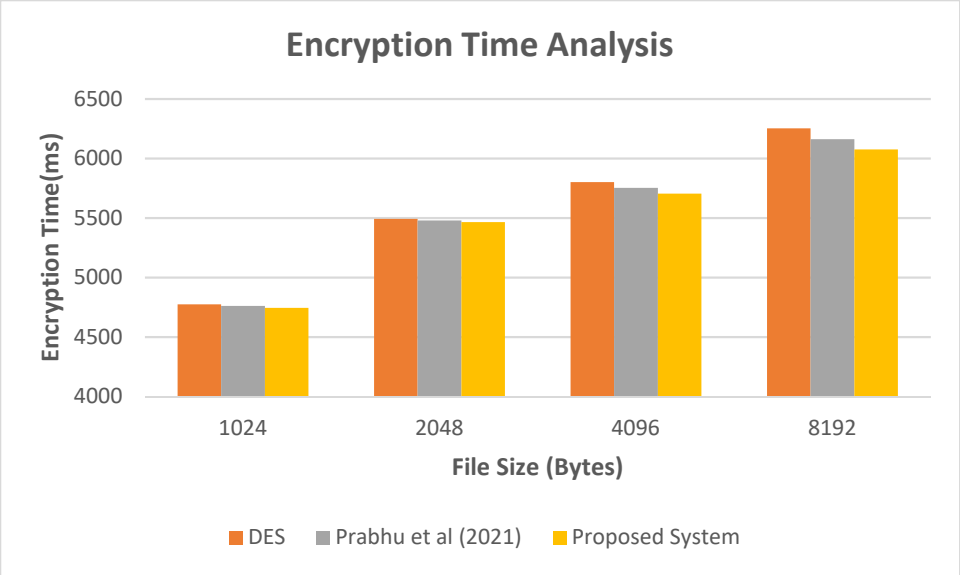

Figure 7. Encryption Time Analysis with different file size

From figure 7, it is proved that the efficiency of the proposed system is better when it is compared with the standard DES and the work done by Prabhu et al (2021) in terms of time taken for performing encryption process on different sizes of files. This is due to the fact that the use of polynomial congruence, ECC and the new key generation technique.

Figure 8 demonstrates that the decryption time analysis by considering the standard DES, Prabhu et al (2021) and the proposed system. Here, the different sizes of files were considered to find the decryption time for performing comparative analysis.

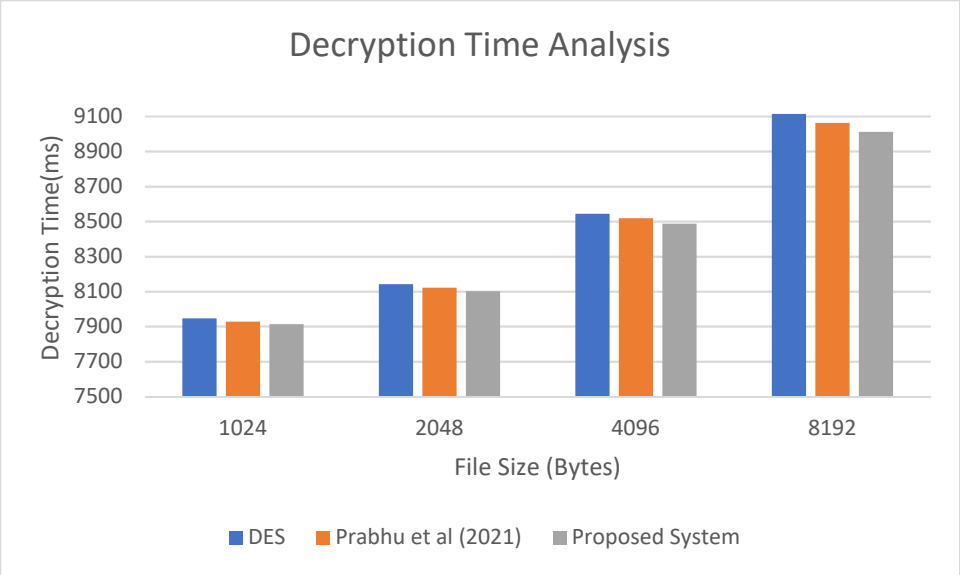

Figure 8. Decryption Time Analysis by considering different file sizes

From figure 8, it is proved that the efficiency of the proposed system is better when it is compared with the standard DES and the work done by Prabhu et al (2021) in terms of time taken for performing decryption process on different sizes of files. This is due to the fact that the use of polynomial congruence, ECC and the new key generation technique.

Figure 9 demonstrates that the encryption time analysis by considering the standard DES, Prabhu et al (2021) and the proposed system. Here, the different sizes of files were considered to find the encryption time for performing comparative analysis.

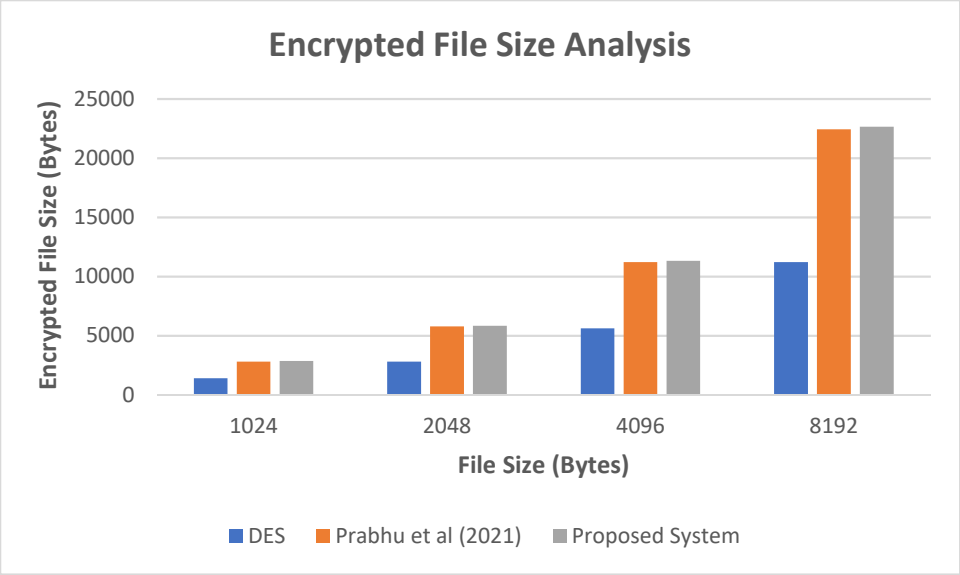

Figure 9. Encrypted File Size Analysis

From figure 9, it is proved that the efficiency of the proposed system is better when it is compared with the standard DES and the work done by Prabhu et al (2021) in terms of encrypted file size that are less from original file size than the standard DES and Prabhu et al (2021). This is due to the fact that the use of polynomial congruence, ECC and the new key generation technique.

Figure 10 demonstrates the security level analysis between the standard cryptographic algorithms such as RSA, AES, DES, ECC, ECC based secured storage mechanism (Prabhu et al 2021) and the proposed secured storage and communication system.

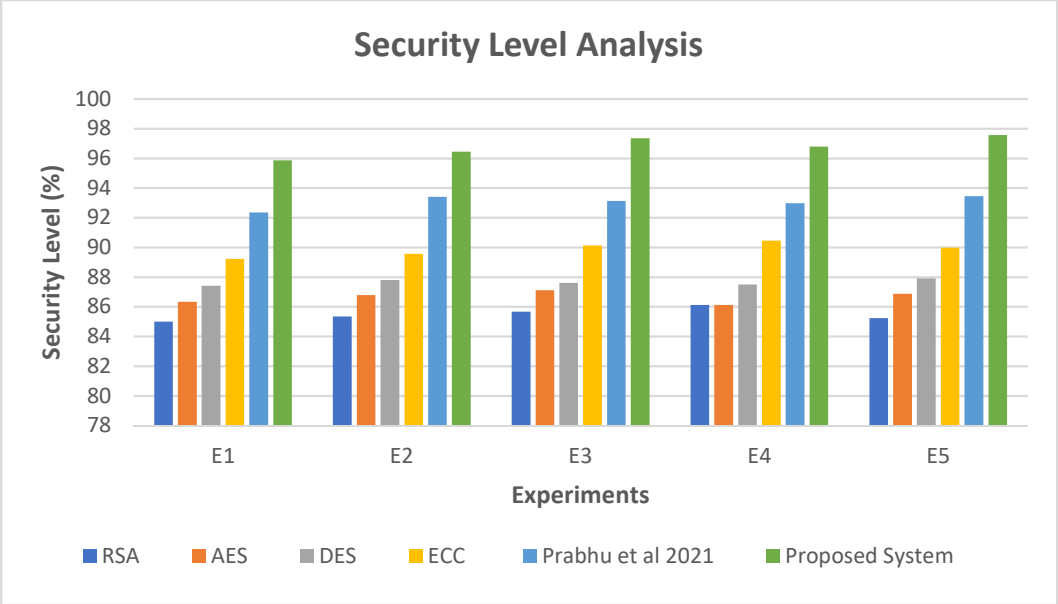

Figure 10. Security Level Analysis

From figure 10, it is proved that the performance of the proposed system is better than the standard cryptographic algorithms such as RSA, AES, DES and ECC, and the ECC based secured storage mechanism (Prabhu et al 2021) and the proposed secured storage and communication system. The reason for the performance enhancement is the application of ECC, Polynomial congruence and the new key generation technique.

6. CONCLUSION AND FUTURE WORKS

A new secured storage and communication system has been proposed and implemented in this work for providing data security while storing the data in cloud database and sharing the data between the cloud users in cloud. The proposed system is built with the combination of prime number generation, key generation for ECC, key generation for DSA, encryption process, decryption process and authorization process. Here, a new technique is introduced to find the alternate prime number which is useful for generating keys for ECC and DSA. Moreover, a new Elliptic Curve and Polynomial Congruence based Encryption / Decryption algorithms have been developed to perform data encryption and decryption in the process of data storage and communication in cloud. Finally, the user authenticity is also performed by applying the proposed digital signature algorithm in this work for storing and accessing the data in cloud. The

experimental results are proved that the efficiency and effectiveness of the proposed system in terms of key generation time, encryption time, decryption time and security level. This work can be enhanced further by the introduction of new encryption and decryption algorithms for providing more security to the cloud data.

DECLARATIONS

Funding: No Funding for this work.

Conflicts of interest/Competing interests: There is no conflicts of interest.

Availability of data and material: Not Applicable

Code availability: -

Authors' contributions: -

Ethics approval: -

Consent to participate: -

Consent for publication: -

REFERENCES

1. V.Pavani, P.Sandhya, Krishna, A. Peda Gopi, V.Lakshman Narayana, "Secure data storage and accessing in cloud computing using enhanced group based cryptography mechanism", Materialstoday:proceedings, 2021.
2. K.Mohana Prabha, P.Vidhya Saraswathi, "Suppressed K-Anonymity Multi-Factor Authentication Based Schmidt-Samoa Cryptography for privacy preserved data access in cloud computing", Computer Communications, Vol.158, pp. 85-94, 2020.

3. Tran Khanh Dang, Chau D.M.Pham, Thao L.P.Nguyen, "A pragmatic elliptic curve cryptography-based extension for energy-efficient device-to-device communications in smart cities", Sustainable Cities and Society, Vol.56, Article No.102097, 2020.
4. Vinod Kumar, Musheer Ahmad, Adesh Kumari, "A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS", Telematics and Informatics, Vol. 38, pp. 100-117, 2019.
5. Sheji Nishoni, A.Aldo Tenis, "Secure Communication With Data Analysis and Auditing Using Bilinear Key Aggregate Cryptosystem in Cloud Computing", Materialstoday: proceedings, Vol.24, No.4, pp. 2358-2365, 2020.
6. Li Yibin, Keke Gai, Longfei Qiu, Meikang Qiu, Zhao Hui, "Intelligent cryptography approach for secure distributed big data storage in cloud computing",Information Sciences, Vol.387, pp. 103-115, 2017.
7. Nesrine Kaaniche, Maryline Laurent, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms", Computer Communications, Vol.111, pp. 120-141, 2017.
8. K.Sowjanya, Mou Dasgupta, Sangram Ray, "Elliptic Curve Cryptography based authentication scheme for Internet of Medical Things", Journal of Information Security and Applications, Vol.58, No. 102761, 2021.
9. S. Atiewi, A.Al-rahayfeh. M.Almiani, S.Yussof et al., "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography," IEEE Access, vol. 8, pp. 113498-113511, 2020.
10. M. M. Potey, C. A. Dhote and D. H. Sharma, "Efficient homomorphic encryption using ECC-ElGamal scheme for cloud data," 3rd International Conference on Electrical, Electronics, Engineering Trends, Communication, Optimization and Sciences (EEECOS 2016), pp. 1-5, 2016.
11. M. Thangapandiyan, P. M. R. Anand and K. S. Sankaran, "Enhanced Cloud Security Implementation Using Modified ECC Algorithm," 2018 International Conference on Communication and Signal Processing (ICCSP), pp. 1019-1022, 2018.
12. P. P. Kendrekar and M. K. Chavan, "Cryptographic implementation of aggregate-key encryption for data sharing in cloud storage," 2016 IEEE International Conference on Recent

Trends in Electronics, Information & Communication Technology (RTEICT), pp. 829-832, 2016.

13. S. Mudepalli, V. S. Rao and R. K. Kumar, "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 267-271,2017.
14. M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in IEEE Access, vol. 8, pp. 52018-52027, 2020.
15. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston and Y. Zhang, "Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications," in IEEE Access, vol. 6, pp. 33552-33567, 2018.
16. X. Yang, M. Wang, T. Li, R. Liu and C. Wang, "Privacy-Preserving Cloud Auditing for Multiple Users Scheme With Authorization and Traceability," in IEEE Access, vol. 8, pp. 130866-130877, 2020.
17. Y. Chen, W. Xu, L. Peng and H. Zhang, "Light-Weight and Privacy-Preserving Authentication Protocol for Mobile Payments in the Context of IoT," in IEEE Access, vol. 7, pp. 15210-15221, 2019.
18. Alrawais, A. Alhothaily, C. Hu, X. Xing and X. Cheng, "An Attribute-Based Encryption Scheme to Secure Fog Communications," in IEEE Access, vol. 5, pp. 9131-9138, 2017.
19. P Elumalaivasan, K Kulothungan, S Ganapathy, A Kannan, "Trust Based Ciphertext Policy Attribute Based Encryption Techniques for Decentralized Disruption Tolerant Networks", Australian Journal of Basic and Applied Sciences 10 (2), 18-26, 2016.
20. B Prabhu kavin, S Ganapathy, "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications", Computer Networks 151, 181-190, 2019.
21. BP Kavin, S Ganapathy, U Kanimozhi, A Kannan, "An enhanced security framework for secured data storage and communications in cloud using ECC, access control and LDSA", Wireless Personal Communications 115 (2), 1107-1135, 2020.
22. BP Kavin, S Ganapathy, "A new digital signature algorithm for ensuring the data integrity in cloud using elliptic curves.", Int. Arab J. Inf. Technol. 18 (2), 180-190, 2021.

23. S Pradeep, S Muthurajkumar, S Ganapathy, A Kannan, "A Matrix Translation and Elliptic Curve Based Cryptosystem for Secured Data Communications in WSNs", Wireless Personal Communications, 1-20, 2021.
24. BP Kavin, S Ganapathy, "EC(DH)2: an effective secured data storage mechanism for cloud based IoT applications using elliptic curve and Diffie-Hellman", International Journal of Internet Technology and Secured Transactions 10 (5), pp. 601-607, 2020.
25. Subbulakshmi Padmanabhan, V. Sumathi, S. Ganapathy, "Cloud based POS System for Secured Smart Shopping CART using RFID", Journal of Advanced Research in Dynamical and Control Systems, Vol.9, No. Sp-14, pp.2764-2777, 2017.