International Journal of Smart Sensor and Adhoc Network

Volume 4 | Issue 1 Article 1

April 2023

A Comprehensive Study on Crypto-Algorithms

Sucheta Panda
Siksha O Anusandhan Deemed to be University, suchetapanda10@gmail.com

Sushree Bibhuprada B. Priyadarshini
Siksha O Anusandhan Deemed to be University, bimalabibhuprada@gmail.com

A Comprehensive Study on Crypto-Algorithms

Cover Page Footnote

The authors are highly grateful to the department of CSE and CS&IT of Siksha 'O' Anusandhan deemed to be university for making this investigation successfully.

A Comprehensive Study on Crypto-Algorithms

Sucheta Panda[1] , Dr. Sushree Bibhuprada B. Priyadarshini [2]

[1,2]Siksha O' Anusandhan University, Bhubaneswar, India

suchetapanda10@gmail.com, bimalabibhuprada@gmail.com

Abstract—In the field of computer network and security, cryptography plays a vital role for secure data transmission as it follows the principle of data confidentiality, integrity, non-repudiation, authentication. By using several cryptographic algorithms, a user can deliver and receive the message in more convenient way. In this paper, we have collaborated on various cryptographic algorithms, several types of cryptographic techniques along with different types of security attacks prevailing in case of cryptography. During the exchanging of any sort of information, the key generation, encryption and decryption processes are examined in more details in the current paper. We have discussed regarding RSA(Ron Rives, Adi Shamir and Len Adelman), which is one of the most secure algorithm in the context of data and information sharing, that has been analysed clearly in our work along with the basic concepts of DES(Data Encryption Standard) , conventional encryption model, ECC(Elliptic curve cryptography), Digital signature, ABE(Attribute based Encryption), KP-ABE(Key policy Attribute based encryption), CP-ABE(Ciphertext policy attribute based encryption), IBE(Identity based Encryption). We have elaborated various cryptograhic concepts for keeping the message confidential and secure while considering secured data communication in case of networks.

Keywords—*Encryption ; Decryption ; Cryptography ; DES; ABE; RSA*

I. Introduction

To communicate securely over insecure networks, three primary concerns must be required: **privacy, authentication, and integrity**. Cryptography is the science of secret writing with the objective of concealing the meaning of a message. **Cryptanalysis** is the study of concepts and strategies for converting an incomprehensible message into the form that can be understood without knowing the key. This process is also known as **code breaking.Crypto protocols** are used to implement cryptographic algorithms. Symmetric and asymmetric algorithms can be thought of as the building blocks for applications like secure internet communication.

A. Symmetric Cipher

A symmetric cipher is one that encrypts and decrypts using the same key. To safely deliver the secret keys to both parties, sophisticated mechanisms are required. **Stream ciphers** and **Block ciphers** [1] are the two types of symmetric ciphers. Data Encryption Standard (DES) and Advanced Encryption Standard(AES) are the examples of Symmetric Cipher. Fig. 1 describes the structure of writing symmetric cipher.

B. Asymmetric Cipher

Ciphers having public and private keys are known as asymmetric ciphers. It has two keys i.e. one for message encryption and another for message decryption. The message can only be decoded by the owner of the second key, according to asymmetric encryption's assumption (that is for the private key, anybody is not aware about it).

A pair of algorithms (E,D) define a symmetric algorithm over (K,M,C).
K represents set of all possible keys.
M represents set of all possible messages.
C represents set of all possible messages.

E: Key(K) X Message(M)
D: Key(K) X Ciphertext(C)
Hence D(K,E(K X M))= Message(M)

Fig.1. Symmetric cipher representation

Likewise, only the public key that corresponds to the private key can decode data encrypted with it. In comparison to symmetric ciphers, asymmetric ciphers are substantially slower. The Diffie-Hellman algorithm, RSA, ciphers, asymmetric ciphers are substantially slower. The Diffie-Hellman algorithm, RSA, and Digital Signature Algorithm(DSA) are examples of asymmetric ciphers.

Fig.2. describes a scenario of asymmetric encryption algorithm and Fig. 3 elaborates about types of Cryptology.

The asymmetric encryption system is made up of three algorithms (H, E, D):

a) H() is a deterministic algorithm that returns a pair of keys(pk, sk)
b) E(pk, m) is a deterministic algorithm that encrypts plaintext m and returns ciphertext c.
c) D(sk, c) is a deterministic algorithm that decrypts c and returns plaintext m.

The following condition must be met for each pair of keys (pk, sk) produced by H and every plaintext message m:

D(sk, E(pk, m))=m

Fig. 2. Asymmetric Cipher

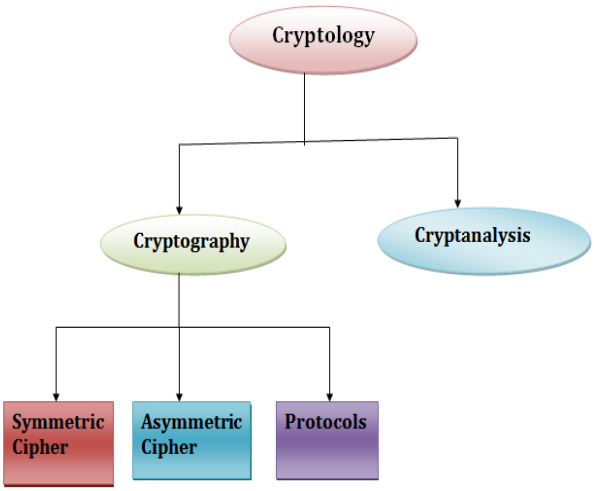


Fig.3. Classification of Cryptology

Cryptography[2]is an area of mathematics that deals with data security, particularly in communications.The following paradigms are used in cryptography:

- **Authentication:** Demonstrating one's identit (common methods of host-to-host authentication are based on name or based on address). Authentication is about validating our secret data. The action of verifying the identity of a user or process is known as authentication.
- **Confidentiality**:Assuring that the communication is only seen by the intended recipient, confidentiality means message must be received by only the intended recipient.
- **Integrity:**Assuring the recipient that the communication it has received has not been tampered with. It is a service ,which ensures that content of the message are not be changed during the transmission.
- **Non-repudiation:**A method of confirming that the communication was sent by the designated recipient. It ensures that original sender of the message can't deny having sent the message.

C. *Applications of Cryptography*

Cryptography is required for communication over any trusted media, which includes the internet.E-commerce, e-payment, e-voting, e-auction and e-gambling all employ cryptographic protocols.

- **Secure communications:** The main purpose of cryptography is to encrypt communication between sender and receiver. This is the most common method of communicating with a server by client software. Example: email client and server , web browser and web server.
- **End-to-end Encryption:** Encryption is rarely used in email. Email is encrypted from server to server and server to user as it passes between them. There are methods to implement "end-to-end-encryption" in email but email systems and solutions both are complex.
- **Storing Data:** Every operating system contains encryption in some of its fundamental components to keep passwords secure, hide specific information and ensuring that updates are actually from the system's developer.

D. *Features Of Cryptography*

- **Confidentiality:** It means that the data is kept secret. That person only can open the text, to whom the sender actually would have sent the data.
- **Integrity:** Data/Information cannot be changed/altered once it is sent to sender.
- **Non-repudiation:** It means the person, who has sent the data cannot deny later about sending that particular data.
- **Authentication:** The sender's and recipient's identities as well as the origin of text both are confirmed.

II. Basic Concepts

Cryptography: The art or science of changing a clear communication into a jumbled message and then restoring that information to its original form.

- **Plaintext**: The message as it was meant to be understood originally.
- **Cipher text**: The message in its new form.
- **Cipher :** An algorithm for converting a comprehensible message into an incomprehensible one by employing transposition and/or substitution techniques.
- **Key :**The sender and recipient are the only ones who know some critical encryption information.
- **Encipher(encode):** The process of employing a cipher and a key to transform normal

message(plaintext) to encrypted message(ciphertext).

- **Decipher (decode):** The process of transforming cipher text into plaintext.
- **Cryptanalysis:** The study of concepts and strategies for converting an incomprehensible message into the one that can be understood without knowing the key (also called as **code breaking).**
- **Cryptology**: Combination of Both cryptography and cryptanalysis.

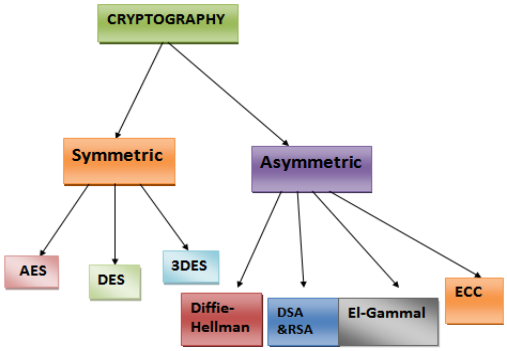


Fig. 4. Types of Cryptography

A. *Types of Cryptography*

Cryptography may be classified into many ways. Fig. 4 describes the types of cryptography briefly. Basically there are 3 types of Cryptography:

1) *Symmetric key Cryptography*

The method in which sender and recipient encode and decode the message by using only single shared key is known as Symmetric key Cryptography. This method is faster and convenient to use. It requires a secure key exchange between the sender and recipient. Example: Data Encryption Standard(DES).Fig.5 represents the Symmetric key Cryptography.

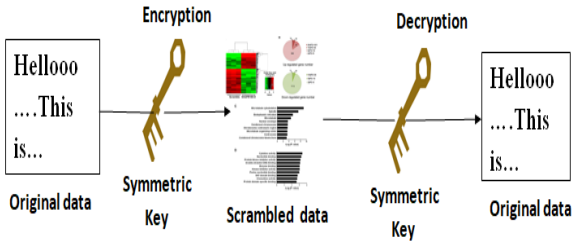
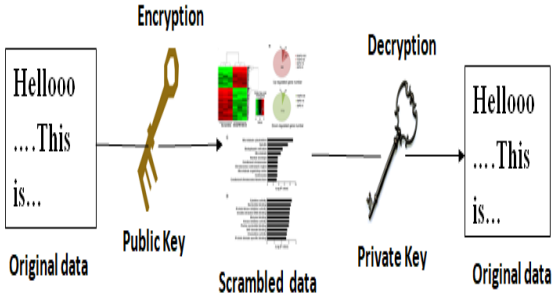


Fig. 5. Symmetric key Cryptography

2) *Asymmetric key Cryptography*



This system encrypts and decrypts data with the help of a pair of keys. For encryption and decryption, public key and private key are used respectively. Public key and Private key are two sorts of keys. Both public key and private key are different in case of Asymmetric key cryptography. Fig. 6. depicts Asymmetric key cryptography.

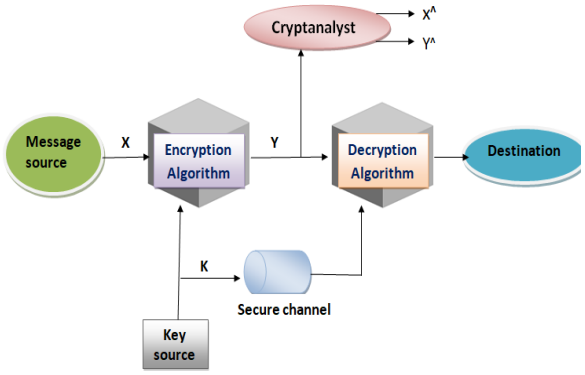


Fig. 6. Asymmetric key cryptography

3) *Dimensions of Cryptography*

Cryptographic systems are classified in three ways:

a) Plaintext to Ciphertext procedure:

Substitution and Transposition in which each plaintext element is replaced with another.

b) The number of keys that are used:

When the sender and receiver use the same key, it is referred to as symmetric key or traditional encryption. It's known as public key encryption when the sender and receiver utilize distinct keys.

c) The method for processing plain text:

A block cipher works with both input and component blocks at the same time, producing output blocks for each input block. In a stream cipher, the input component is processed in real time, with each output element being created one at a time.

III. SIMPLIFIED MODEL OF CONVENTIONAL CRYPTO SYSTEM

Traditional encryption[3] is a cryptographic technique that encrypts and decrypts messages using the same key. It was the only technique of encryption accessible prior to the development of public-key cryptography.Because of its simplicity, it is still the more popular of the two encryption schemes. Because it employs the same key for encryption and decryption, it is a rather quick operation. The sender encrypts plaintext with the recipient secret key, which the receiver can then use to decrypt the ciphertext. This concept is depicted in Fig. 7.

For example,Alice wishes to send Bob a message; this message is known as plaintext. To prevent hackers from reading plaintext, it is now encrypted with an algorithm and a secret key. Ciphertext is the name given to the encrypted plaintext. B can decrypt A's plaintext using the same secret key and reverse-encryption technique, allowing the message to be read and security to be preserved. This technique is based on an old notion, which is why it is known as conventional encryption.

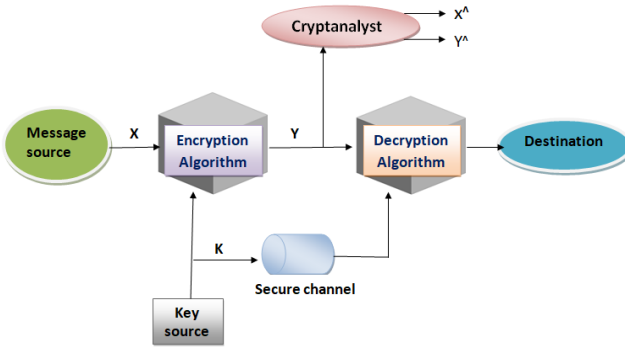


Fig.7. Conventional Crypto Model

There are five key components to traditional encryption:

- **Plain text:** As an input, the algorithm receives the original data.
- **Encryption algorithm:**This encryption algorithm transforms plain text into ciphertext through a series of modifications.
- **Secret key:**The algorithm accepts the secret key as an input. Based on the keys used at the moment, the encryption method will generate different results.
- **Ciphertext:**It transmits encrypted data as it comprises a version of original plaintext that cannot be decrypted by a human or a computer without the use of the appropriate cipher.
- **Decryption algorithm:**This is employed in the decryption of encryption methods. It accepts ciphertext and a secret key as input and produces plaintext as output.

A. Conventional Encryption's Benefits

- **Simple:**This sort of encryption is simple to use.
- **Reduces the amount of computing resources required:**When compared to a public key encryption, traditional encryption does not necessitate a lot of computer resources.
- **Fast :**Traditional encryption is much slower than asymmetric key encryption.

B. Traditional Encryption's Model's Drawbacks

- Because both sender and recipient share the same key, the origin and authenticity of the message cannot be ensured. Messages from specific user can not be confirmed. In comparison to public-key encryption, it isn't very secure.
- Users will be unable to decrypt the message, If the receiver misplaces the key. So, rendering the entire process is meaningless.
- As both the sender and recipient must agree on a secret key before transmission, the system does not scale effectively to a large number of users.

IV. DIGITAL SIGNATURE

The electronic equivalent of a physical signature is a digital signature[4], which is based on public key cryptography. Diffee and Hellman proposed it in 1970.

- In the absence of a physical signature, a digital signature [5] is employed to validate the message's legitimacy.
- Message authentication is true if the person can generate a valid digital signature of the original message.

- The sender's private key and the message being sent are used to create a digital signature.
- Digital signature are verified using the sender's public key[6].

It requires the usage of two functions as follows:

a) Digital signature signing function:-

$$Y=\text{sig}K_{PR}(x)$$

b) A digital signature verification function:-

Ver K_{PUB}=(x,y)≡True or False,If true then select, otherwise reject.

A digital signature must provide:

- Authenticity and integrity
- Non-repudiation

Because signing (encrypting using a private key) takes a long time (and takes up a lot of space), prior to encrypting messages, we usually include a time (and a space) saving step. It's known as hashing or message digestion.

V. PRELIMINARIES

A. *Cyclic Group*

Every element of a cyclic group[7] is a power of a fixed element. If $G =< g >$ for some$g \in G$, then the group G is cyclic. $g$is a generator of $< g >$. $G =< g >$ is cyclic of order n if g has order n. $G =< g >$ is infinite cyclic, if a generator g has infinite order.

B. *Finite field*

A set having finite number of elements is called a finite field. The set of integers modulo is an example of a finite field. There are two binary operations available in fields: addition (+) and multiplication (•). Both are associative, commutative, and closed. There is a unique identity element for both operations, and a unique inverse element for each element. Last but not least, multiplication is distributive over addition.

C. *Symmetric Pairing*

LetG, G_T stand for prime order r cyclic groups. Suppose g be a generator of G.

A bilinear pairing is also known as bilinear map, is a function that is easily computed. That is;

$$\boldsymbol{e}: \boldsymbol{G} \times \boldsymbol{G} \rightarrow \boldsymbol{G_T}$$

Such that

a) **Nondegeneracy**: $e(g,g) \neq 1$

b) **Bilinearity:** $e(g^a, g^b) = e(g,g)^{ab}$ for all $a, b \in Z$.

The value it takes at $e(g,g)$, completely defines an asymmetric bilinear map. For any given cyclic group, there is only one bilinear map: When $e(g,g) = 1$,we have a degenerate situation, whereas all other $r-1$ maps are equal upto a constant.

We can instantly how effective the power of such a map. g, g^x, g^y, g^z given by bilinearity and non degeneracy, $z = xy$ if and only if $e(g, g^z) = e(g^x, g^y)$. To put it another way, the Diffie Hellman problem can be resolved.

VI. ELLIPTIC CURVE CRYPTOGRAPHY(ECC)

ECC is a public key encryption system based on the algebraic structure of elliptic curves in finite fields. In 1985, Victor Miller and Neil Koblitz developed Elliptic curve cryptography as a replacement for public key encryption. Elliptic Curve Cryptography (ECC) [7] is a new public-key encryption system that is smaller, faster, and more efficient than its predecessors.Rather than using the usual approach of creating keys as a product of very large prime numbers, ECC uses the features of elliptic curve equation to produce keys. Fig.8. shows the concept of Elliptic curve Cryptography. The equation for an elliptic curve is:

$$y^2 = x^3 + ax + b$$

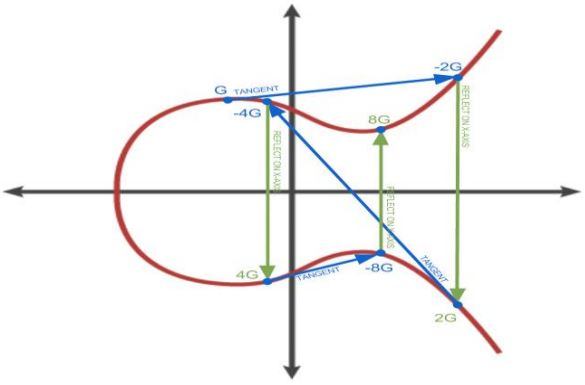


Fig. 8.Elliptic Curve Cryptography

There will be a few terminologies used that will be utilized:

E -> **Elliptic curve**

P -> **Point on the curve**

n -> **Maximum limit (** prime number**)**

*A.**Key Generation :***In key generation procedure, we must generate both a public key and private key. The communication will be encrypted with the sender's public key and decrypted with the receiver's private key. We must now select a ‘d’ from the range of ‘n’ numbers. The equation is shown below can be used to produce the public key.

$$Q = d * p$$

$\boldsymbol{d} =$ We chose a random number from a range of possibilities$(1\ ton - 1)$. P is the curve’s starting point.

'Q' **public key**
'd' **private key.**

B. **Encryption**

Let’s take ‘m’. On the curve, we need to depict this message. This document contains comprehensive implementation information. Certicom is the company that does all the advanced research on ECC.

Let’s take the case where 'm' has the 'M' point on the 'E' curve. Pick 'k' at random from the range $[1 - n - 1)$.

$C1, C2$ are the two ciphertext that will be created.

$$C1 = k * P$$

$$C2 = M + k * Q$$

$C1\ and C2$ will be sent.

C. **Decryption**

We need the message’ m’ that was sent to us to be returned to us.

$$M = C_2 - d * C_1$$

M stands for original message we sent.

VII. DISCRETE LOGARITHMS IN FINITE FIELDS

The discrete logarithm issue was suggested by Diffie and Hellman in 1976 as a safe key exchange scheme (DLP). Discrete logs appear in the context as aids for determining where a particular block occurs in a shift register sequence. However, the advent of the Diffie-Hellman method [8] provided the primary motivation for the current surge in interest in discrete logs. In the world of cryptography, DLP is one of the most important issues [9]. Many DLP-based cryptosystems, including Diffie-hellman transfer cryptogram protocol[10], the Okamoto Conference-key sharing technique[11], Elgamal Public key crypto system[12], & others have been proposed for establishing PKI system. We have to compute g^uzfromg^uandg^z without knowing x and y. Fig. 9. shows the work details of Discrete algorithm.

S={1,2,3,…,q-1}

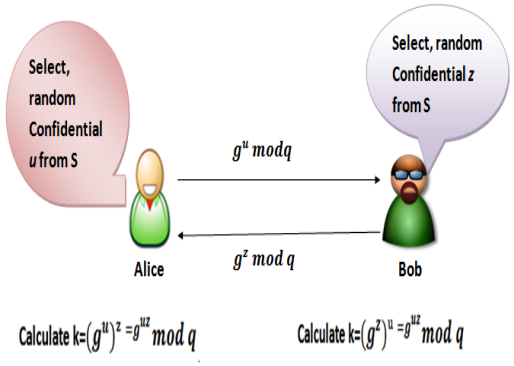


Fig. 9. Discrete Logarithm

VIII. BILINEAR MAP

The bilinear map is the most common pairing based construct. Consider the prime order p and groups G_1, G_2, G_T . The elements g_1 ЄG1 and g_2 ЄG2. Where g_1 and g_2 are the generators of G_1, G_2 respectively. A bilinear map $e: G_1 \times G_2 \rightarrow G_T$. The properties are :-

- Bilinearity: $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$,for all g_1Є G_1 and g_2ЄG_2 ,where a,b Є Z_p.
- Non degeneracy: There exists g_1 Є G_1 , g_2Є G_2 ,such that e(g_1 , g_2)≠ *1*. To put it another way, the maps donot send all of the pairings in $G_1 and G_2$ to the identity in G.

Computability: For all $g_1 \in G_1$ and $g_2 \in G_2$ [4,10], there is an efficient procedure for computing $e(g_1, g_2)$.

IX. RON RIVES, ADI SHAMIR AND LEN ADELMAN(RSA)

The R.S.A algorithm was developed by Ron Rives, Adi Shamir and Len Adelman in 1978. This scheme makes use of an expression with exponential. It's commonly used for digital

signatures and key distribution. This method employs an exponential expression. Shireen Nisha [13] aims to analyze RSA, examines its virtues and shortcomings, and provides new techniques to address the flaws in her work in this study. Rivest, Shamir, and Adleman (RSA) is a cryptographic method for ensuring secure network communication.The RSA cryptosystem is built on the assumptions that determining factors for large integers which is difficult. It includes supplying publickey and privatekey to the sender and recipient in order to encode and decode the message [14]. **Key creation**, **Message encryption**, and **Message decryption** are the 3 steps in the RSA process.

RSA Algorithm

We can produce encryption and decryption keys in the following way:

Step-1 : Make two huge primes at random using $pandq$.

Step-2 : Calculate $n = pq$ and $\varphi = (p-1)(q-1)$.

Step-3 : select a number e , so that $gcd(e,\varphi) = 1$.

Step-4: Calculate the m$ultiplicativeinverse$ of e modulo φ to find d.

So that$ed \equiv 1(mod\Phi)$, which is done efficiently using Eulid's Extended Algorithm.

The public key for encryption is$K_E = (n,e)$and the decryption private key is $K_D = (n,d)$.

Step-5 : The encryption function is $E_M = M^e$mod n. The decryption function is $D_M = M^d$ mod n.

These functions satisfies$D(E(M)) = M$ and $E(D(M)) = M$ for any $0 \leq M < n$.

A. Prime numbers , Factorization and Eulear'sTotient Function

The ancient Greek mathematician was well-versed in prime numbers and their properties. To answer the challenge, different properties of integers are identified. A positive integer that has no divisors and that can only be divided by one and itself is known as prime number.

Factorization of integers are generally in the form g=f1× $f2 \times \ldots \times fn$ or g=-1× f1× $f2 \times \ldots \times fn$

Where f_i is a prime < 1 $andfi \leq fjfori < j$.

For example:$g = 72$ and its factors in the form -1 $\times 2 \times 2 \times 2 \times 3 \times 3$. The positive integer numbers , or not greater than n, and relatively prime with n ,equals to Eulear's totient function $\varphi(n = \{\alpha|N: 1 \leq \alpha \leq nand\ \gcd(\alpha,n) = 1)$.

X. CP-ABE IN CLOUDCOMPUTING

Attribute-based encryption protects users' privacy by using a collection of attributes. Because the cloud is now widely used in almost all industries, there is a need to maintain data that is outsourced on the cloud as more secure and confidential. Data security on cloud database servers is a major cause of concern when it comes to cloud adoption. It necessitates a high level of secrecy and authentication. CP-ABE is frequently used as a data protection approach in cloud computing because of its scalable and flexible characteristics for access control on a finer scale. The access policy on the other hand contains sensitive information in CP-ABE scheme, exposing the privacy of the data source of receiver. Each user in CP-ABE is given a set of qualities which can be used to build a secret key. A set of rules is also used to generate the ciphertext. Only if the properties associated with a secret key meet the policy described in the ciphertext can it be utilized to decrypt the ciphertext[15].

XI. HISTORY OF DATA ENCRYPTION STANDARD(DES) ALGORITHM

DES is a symmetric block cipher created by National Institute of Standards and Technology(NIST). In 1973 NIST issued a request for proposals for a national symmetric key encryption. The DES block cipher converts plaintext to ciphertext using keys of 48 bits. It uses a symmetric key algorithm which means it encrypts and decrypts data with same key. Because of the key length(56 binary) used to generate the other keys , the DES algorithm isconsidered dangerous. The DES algorithm is essential for research because it ensures security and confidentiality. Fig. 10. Shows the structure of DES process[16].

A. Applications of DES

- The US government made the DES algorithm essential for all financial operations including computerized fund transfer.
- ATMs with high speed.
- It is a secure video teleconferencing system.

- Routers and remote access servers contain it.
- When sensitive information requires cryptographic protection, federal departments and agencies can employ it.

Input

8-bit plaintext(10111101)

10-bit key(1010000010)

Output: 8-bit Cipher text.

Functions

IP : Initial Permutations

f_K: Function involving permutation and substitution with key.

SW : (Switches) a simple permutation function.

IP^{-1}: Inverse of IP

Encryption Scheme

Cipher text= $IP^{-1}(f_{k_2}(SW(f_{k_1}(IP(plaintext)))))$

$Where \quad K_1 = P8(Shift(P10(key))$

$K_2 = P8(Shift(Shift(P10(key)))$

Decryption Scheme

Plaintext=$IP^{-1}(f_{k_1}(SW(f_{k_2}(IP(Ciphertext)))))$

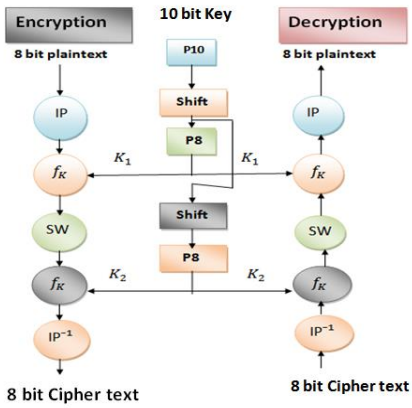


Fig. 10. DES process

XII. PUBLICKEY CRYPTOGRAPHY(PKC)

PKC is another name for Asymmetric key encryption. It encrypts and decrypts data using public and private keys[17]. The keys are nothing more than two massive numbers that have been matched but are not similar. One of the keys in a pair that may be shared with anybody is called a publickey. The pair's other key that is private key is kept hidden. A message can be encrypted with any of the keys; the decryption is the inverse of the one used to encrypt the message. Even for key exchange, PKC is often used to secure electronic communication over a public network such as Internet, without relying on a secret or covert channel.

A public key cryptosystem[18] consists of two keys:

- Encrypting key
- Decrypting key.

Although the two keys perform opposite functions and are thus related, there must be no simple way to derive the decrypting key from the encrypting key. Thus the encrypting key can be made public without imperil the decryption key, allowing everyone to encrypt communication but only the intended recipient to decrypt it. Fig. 11. describes the Public key Cryptography concept.

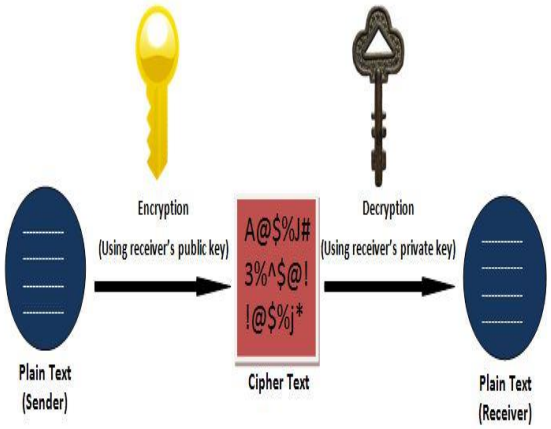


Fig. 11. Public Key cryptography

XIII. ATTRIBUTEBASED ENCRYPTION(ABE)

In ABE scheme attributes play very important role to control users access. It is a type of Public key cryptography, that uses pair of keys : public and private. Public keys are available in publicly and private keys are only known to the owner. ABE is a system that combines PKC and IBE. The ABE scheme assigns a set of properties to both the ciphertext and the key. The encryptor can devise an encryption method based on the information's characteristics and the receiver's characteristics and the ciphertext generated can only be decrypted by users whose characteristics

are compatible with the encryption policy. Attribute based encryption has two main benefits:

1. It has advanced access control capabilities.
2. The scheme does not allow to remember the number of users to access the document .

An important policy of ABE scheme ,it satisfies the collusion resistance. It's suitable for a variety of purposes, including distributed file management and third-party data storage[19].Collusion resistance indicates that the encrypted text is decrypted by two or more users who have separate keys. They will be successful if and only if each of the users can decrypt separately. It means that unless one of the users able to decrypt the ciphertext, they should not able to decrypt it. This features ensures that only those with the correct key have access to the data. Depending on the access policy incorporated in the ciphertext or the user's secret key, the system is classified into two categories such as CP-ABE[20] and KP-ABE.

The following are the four major phases that makeup an ABE scheme. Fig. 12. briefly describes the steps of ABE scheme and Fig. 13 explains about ABE procedure.

Step-1: Setup (k, U)

For this algorithm the input restrictions are the security parameter and the Universe of the attribute U. The primitives create a master key MK based on the domain parameters PK.

Step-2: Encryption (PK, M, A)

This technique takes a set of domain parameters PK, a message M and a access policy A as a Boolean formula with operands that are a subset of universe of attributes as input. M is then encrypted as the ciphertext CT, which can only be decrypted by the users who have set of attributes required to meet the access policy A. It is assumed that the ciphertext and accesspolicy A will be sent together.

Step-3: Key generation (MK, S)

The masterkey MK and a collection of characteristics S are utilized as input in this operation. After that the private key SK is produced with the necessary attributes. This primitive is typically carried out by a "trusted third party" who is in charge of generating private keys for each of the participants with varied access privileges.

Step4: Decryption (PK, CT, SK)

This primitive accepts the domain parameters PK, ciphertext CT and its associated access policy A, as well as the private key SK which contains the set of attributes S. Only if the collection of features 'S' satisfies the policy A will this primitive be able to retrieve the message M from the ciphertext CT.

Fig. 12. ABE algorithm

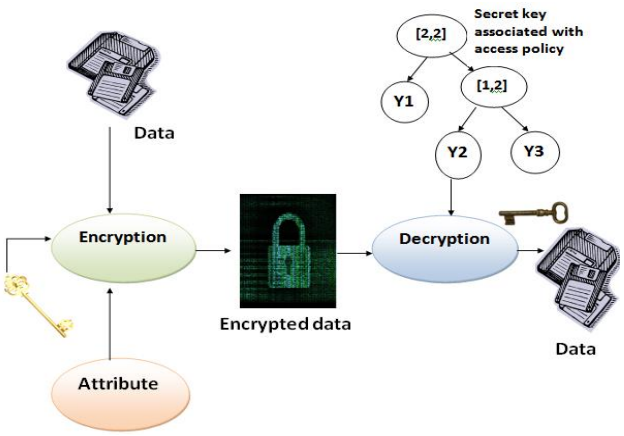


Fig. 13. Attribute Based Encryption process

Categories of Attribute based Encryption:It helps to group logically into three versions in order to comprehend the possibilities of Attribute based Encryption.

a) Access Control based on Content

When encrypting sensitive data in an ABE system, attributes for content-based access control will be linked to a ciphertext. A private key will be associated with a policy over these attributes on the IP side; the policy is commonly represented as a Boolean formula.(This variety is also known as "key-policy" ABE in academic literature).For instance, in an email encryption system, we might extract the To and From address as characteristics as well as the time sent and subject while encrypting the email body as secret data.

b) Access Control based on Role

A private key will be linked to attributes and the ciphertext will be linked to a policy(or Boolean formula).The qualities will frequently be linked to a private key holder's credential in such system.(This version is also known as(CP-ABE) in academic literature[16].

c) Multi-authority Role based Access control

One challenge with role-based access control is that we would like to develop access control policies that span multiple administrative boundaries in various applications. One drawback of regular ABE is that it only allows one authority to distribute private keys. However, it is natural for various authorities to handle different qualities in many applications. ABE is categorized into two types described below.

XIV. CP-ABE

Today, the CP-ABE is the most useful. It accepts arbitrary schemes and attributes, as well as numerical keys attributes. The ability to organize attributes into sets, as well as a frame policy that restricts the decrypting key selectively. Identity Based Encryption can be considered a generalization of CP-ABE. For constructing more limited keys a single publickey and a masterkey are utilized in IBE. CP-ABE is more flexible than IBE. Each CP-ABE is assigned asset of attributes from which her private key is generated. The encryptor defines an access structure for encrypting the message 'M' in terms of a set of given properties. The message can only be decoded by those who have attributes that match the access structure. Unauthorized users will be unable to decode the encoded text evenif they collaborate.The following are the four phases that makeup the CP-ABE scheme. Fig. 14. describes the steps of CP-ABE scheme.A representation of CP-ABE is shown in Figure 15. Each user has their own collection of traits. Only User 3 has the ability to decrypt the data because his or her features match the ciphertext's access tree requirements <Mumbai OR Rajesh AND Clerk>.

1. Setup: This method accepts a security parameter input and outputs the public key PK as well as the system secret master key MK. Message senders encrypt their messages using PK. The authority has access to MK, which is used to generate user secret keys.
2. Encrypt: The public parameter PK, a message M, and an access structure T are all inputs to this algorithm. It generates the CT ciphertext.
3. Key-gen: The master secret key MK, as well as a set of user specific properties are used as input in this method. It creates a secret key SK that allows the user to decrypt a message encrypted with access tree structure T if and only if it meets certain criteria.
4. Decrypt: For an attributes set, this algorithm accepts the ciphertext CT and a secret key SK as inputs. It returns the message M if and only if the access structure associated with the ciphertext CT is satisfied.[22]

Fig. 14. CP-ABE Algorithm

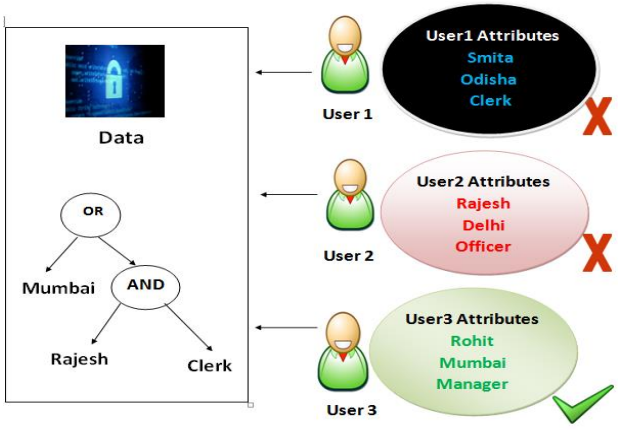


Fig. 15. Schematic Overview of CP-ABE

CPABE scheme [21] work in the reverse in the sense that in CP-ABE , policy structure are embedded in data and attribute in keys. Boneh proposed Hierarchical Attribute based Encryption(HIBE) system which includes efficient encryption time and forward secure encryption. The CP-ABE scheme proposed by Bobba et al. first organize user attribute in keys and allows user to report dynamic constraint on attributes to satisfies policies. This allows the scheme flexible and efficient when supported with complicated attribute. A lightweight CP-ABE method was presented by Touatiet [22].A symmetric key is used first to encrypt the data in the suggested method. The ability to limit data access is the major difference between KP-ABE and CP-ABE. Data in KP-ABE is simply comprised of user attributes, and anyone can access it. Because the access tree is encrypted, CP-ABE on the other hand may control data access. Han et al. [23] presented a decentralized ciphertext-policy attribute-based encryption system that maintains privacy in order to promote security and privacy. Fig. 15. shows the process of CP-ABE scheme.

xv.KP-ABE

It's a variant of ABE's encryption method. KP-ABE is a 1-to-n communication system that supports for fine-grained encryption data sharing. Every cipher-text is given a set of descriptive qualities in this system. The access structure, also known as policy, is captured using the user's secret key, which is issued by a trusted authority. Goyal et al. [24] first time presented the KP-ABE structure which allowed monotonic formula to be used to construct access restrictions in encrypted data. The system was determined to be selectively secure using the Bilinear Diffie-Hellman assumption. Ostro-vsky et al.[25] created a KP-ABE system in which private keys can reflect any access formula over attributes, even non-monotone ones. Goyal et al. included revocation procedures into Goyal et al. in KP-ABE scheme. Chang-ji wang presented a new KP-ABE with a fixed ciphertext size. Any monotone access structure in our implementation can be defined as the access policy. Fig. 16. Represents the steps of Key Policy Attribute Based Encryption concept and Fig. 17. Shows the process of KP-ABE

scheme.The following are the four algorithms that makeup the KP-ABE scheme.

Users have access to a tree of keys that can be used to identify attributes, and each Data has its own set of attributes (such as Name, Location, or Service type). Only when data met the access tree's requirements was it decrypted with the access tree. An access tree looks like this: <Mumbai OR Rajesh AND Clerk>. Each of the three data points has three characteristics that correspond to Name, Location, and Service Type. A user can then only decrypt Data 3 depending on his location (Mumbai). Due to the fact that the user key is an access tree, KP-ABE doesnot have the authority to check data access[26].

1. Setup: This algorithm, which accepts a security parameter as input, returns the public key PK, and the system master secret key MK. Message senders use PK to encrypt their messages. MK, which is used to create user's secret key is accessible to authority.

2. Encryption: This method takes three inputs: the message M, the public key PK, and a collection of characteristics. E is the ciphertext that is generated.

3. Key Generation: This algorithm takes two inputs: the access structure T and the master secret key MK. It produces a secret key SK that allows a user to decrypt a message encrypted using a set of attributes if and only if equals to T. This technique only displaces the message M, if the attribute set matches the user's access structure T.

4. Decryption: For access structure T, it accepts the user's secret key SK and the ciphertext E, which was encrypted with the attribute.

Fig. 16. Schematic Overview of KP-ABE

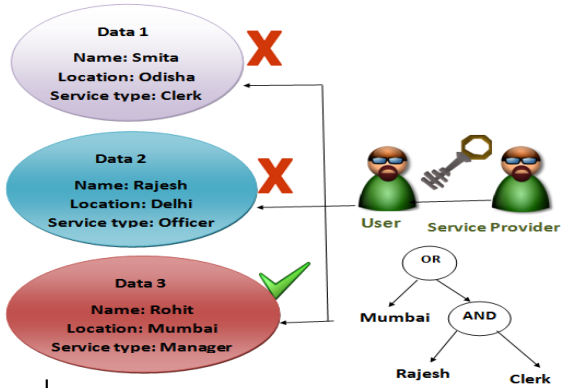


Fig. 17. Key Policy Attribute Based Encryption(KP-ABE)

XVI. COMPARISION BETWEEN KP-ABE AND CP-ABE

In comparision to KP-ABE, the CP-ABE system is quite efficient.Because CP-ABE puts access policy decisions in the hands of data owner, it is more appropriate for data sharing.It mitigates the shortcoming of KP-ABE, which is that the encrypted data has no control over who decrypts it.Fig. 18 explains the difference between KP-ABE and CP-ABE and the following Table.1 shows the comparative analysis of between them.

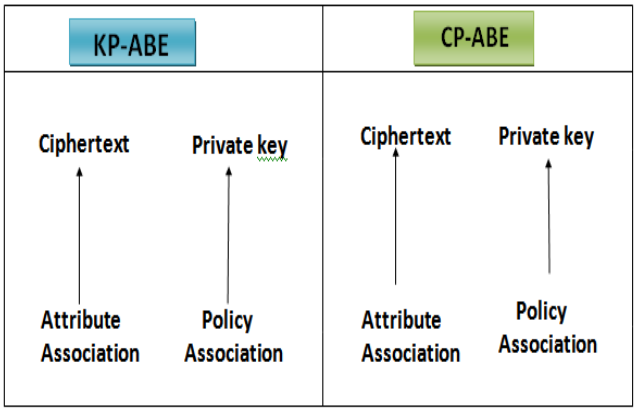


Fig. 18. Comparison of KP-ABE and CP-ABE

TABLE I. COMPARATIVE ANALYSIS BETWEEN KP-ABE AND CP-ABE

PARAMETERS	KPABE	CPABE
ACCESS CONTROL	LOW	HIGH
EFFICIENCY	AVERAGE	HIGH
SECURITY	AVERAGE	HIGH
COLLUSION RESISTANT	HIGH	HIGH
COMPUTATION OVERHEAD	HIGH	AVERAGE

XVII. IDENTITY BASED ENCRYPTION(IBE)

Adi Shamir was the first to propose IBE. IBE is a crucial part of an Identity based cryptography. IBE is a sort of Public key encryption in which a user's public key is derived from identity related attributes, for example: *email address*. It implies that a sender with access to the public parameters can encrypt a message using a key such as the recipient's name or the text value of the recipient's email address. Any party in an Identity-based system can generate a public key from a known identity value, such as an ASCII string created by the author.

Identity based Encryption is less versatile than CP-ABE. Every user in CP-ABE is allocated a set of attributes from which she can generate her private key. The encryptor specifies an access structure for encrypting message M using a set of specified characteristics. Only those with attributes matching the access structure can decode the message. Even if they work together, unauthorized users will be unable to decrypt the encrypted text.Kapadia et al.[27] presented a scheme which has the same flexibility and implements hidden access structure.This scheme restricts collusion of user secret keys. A single public key and master private key are used in Identity based encryption to create more limited keys.Clifford Cocks presented an IBE system employing the quadratic residuosity as his underlying primitive in the Clifford Cocks presented an IBE system employing the quadratic residuosityas his underlying primitive in the same year as Boneh and Franklin [28].Fig. 19 and Fig. 20 describe the process of IBE scheme.

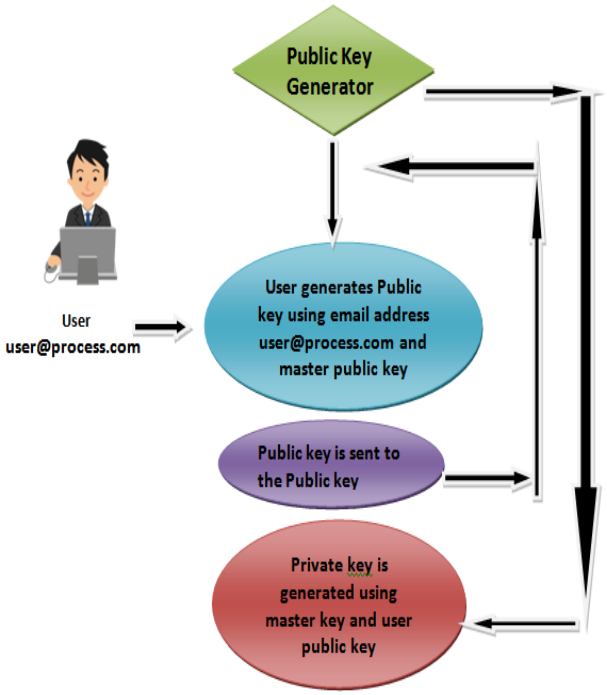


Fig.19. Identity based Encryption Diagram

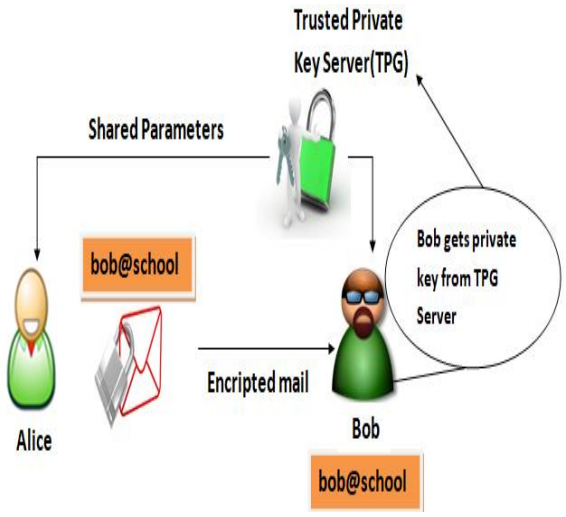


Fig. 20. Instance of IBE

The diagram above indicates that messages are encrypted for an identity, and the user simply has to know recipient's identity. Example:personC@pkg.com.

A. Advantage

• There are no requirements for certificates. The identity of a recipient is used to generate his public key.

• There is no need to sign up ahead of time.

• Keys do not have to be revoked because they expire. When keys are compromised in a standard public-key system, they must be revoked.
• Spam is less likely.
• Allows messages to be postdated and decrypted later.
• Allows for automated expiration of communications, rendering them illegible after a set period of time.

*B.**Disadvantage***
• A centralized server is required. Because of IBE's centralised method, some keys must be created and stored in escrow, putting them at danger of being exposed.
• The private key must be transmitted over a secure connection between the sender and the IBE server.

XVIII. FUZZY IDENTITY BASED ENCRYPTION:

A person's fuzzy identification is a collection of descriptive characteristics with a predetermined error tolerance capability. These qualities serve as a public key in Fuzzy-IBE. Fuzzy-IBE is the next step in the evaluation of Identity Based Encryption systems, which includes an error-tolerance element. We employ the error-tolerance function in IBE systems that use biometric identities since it is more convenient. The idea stemmed from the fact that biometric scans are never completely accurate and always include some noise. In Fuzzy IBE, an identity is considered as a set of descriptive features. A ciphertext encrypted with an identity can be decrypted with a private key for that identity.

In a Fuzzy IBE scheme if and only if the identities are measured by the ”set overlap” distance metric. Sahai and Waters[29] describe a technique for associating encoded messages and private keys with a set of attributes. Only the user should be able to decrypt the ciphertext if the ciphertext’s properties coincide with the attributes associated with the user’s private keys.

Identification is represented as a set of descriptive values in Fuzzy IBE, and a user with the IDA private key can decrypt a ciphertext encrypted with the IDA private key and can decrypt a ciphertext encrypted with the IDB public key if and onlyif the overlap between IDA and IDB satisfies the predetermined threshold value. Therefore, Fuzzy IBE possesses a crucial quality known as error-tolerance.[30].Yao et al. [31] describe how a forward safe Hierarchical IBE method is implied by an IBE system that encrypts to multiple hierarchical identities in a collusion-resistant way. They also mention how attribute-based encryption can benefit from their strategies for preventing collusion attacks. As the number of attributes increases, the cost of their method grows exponentially in terms of computation, private key size and ciphertext size[32].

Based on the Baek et al. technique , a biometric IBE strategy was proposed in [33],which is more efficient at encrypting and produces shorter ciphertext than earlier methods. Fig. 21 shows the setup and keygeneration phase of Fuzzy Identity based Encryption. Fig. 22 describes the process of Encryption and Decryption phases of Fuzzy Identity based Encryption.

*A.**Setup and Key Generation:***

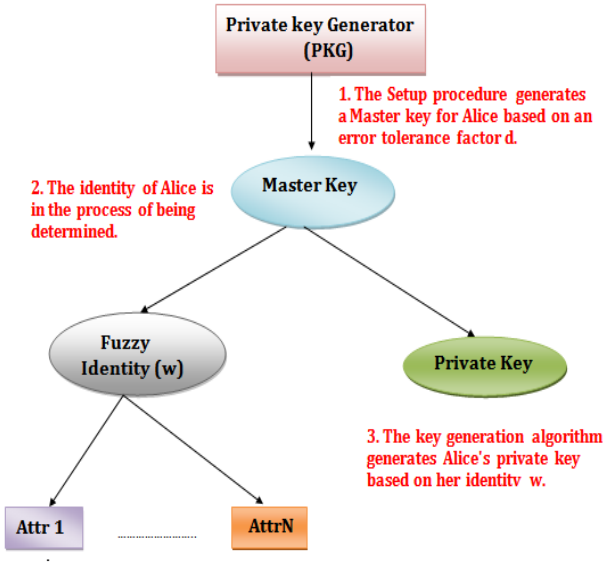


Fig.21. Setup and Key generation phase

B. Encryption and Decryption

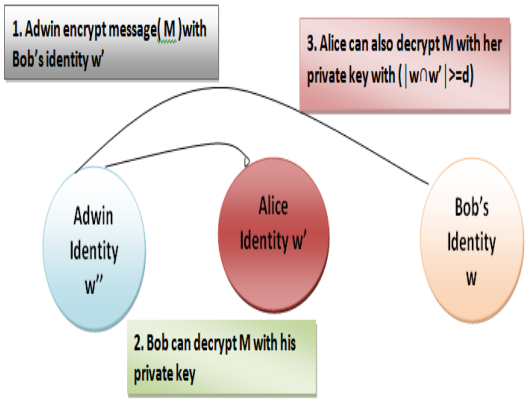


Fig.22. Encryption & Decryption phase

XIX. ACCESS STRUCTURE

An access policy is one that specifies the types of people that are allowed to read the documents. For example, in an academic context, a professor in charge of the course and a few teaching assistants (TAs) may have access to a class's grade sheets. As shown below, the access policy can be expressed as a predicate.Fig. 23 describes an example of access structure policy.

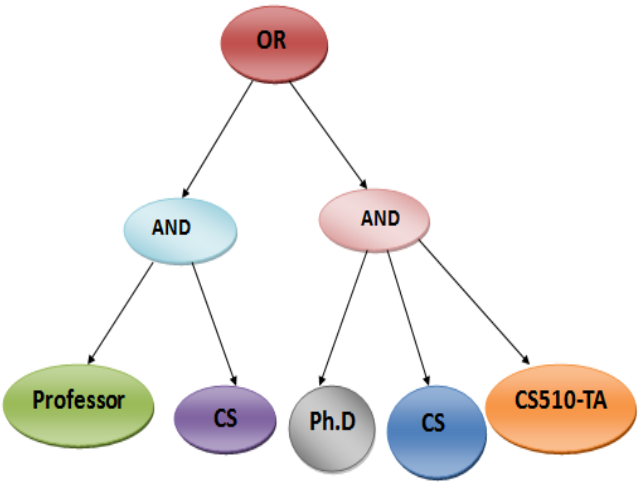


Fig.23. Access Structure example:[((Professor ∧ CS) V (M.Tech ∧ CS ∧ CS410-TA))]

A.Thresold Predicate

In thresold access poicy structure,suppose bob wishes to encrypt and transmit a message to persons who have atleast 3 of the 6 characteristics listed below.Fig. 24 depicts thresold predicate.
The attributes are:
{Reetam,Teacher,School,Mathematics,Student,Physics}

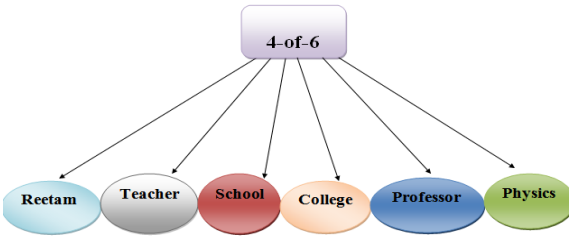


Fig. 24. Thresold Predicate

AND gate : $n - of - n$ thresold gates.
OR gate: $1 - of - n$ thresold gates.
Policies can be established using conjuctions, disjunctions and (k, n) threshold gates, which require that $k\ out\ of\ n$ attributes be present. Let's say the universe of attributes is specified as $\{A, B, C, D\}$ and that first user gets keys to attributes $\{A, B\}\ and\ \{D\}$, where as user 2 receives a key to attribute D. User 2 will be able to decrypt a ciphertext encrypted using policy (A∩ C)∪ D but not user 1.Fig. 25 describes the structure of Thresold gates.

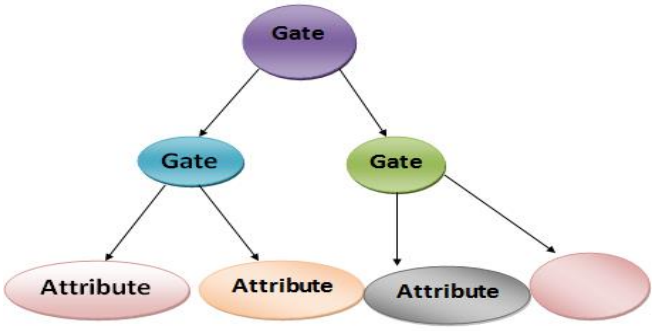


Fig. 25. Thresold gate

XX. SECURITY ANALYSIS OF ABE TECHNOLOGY

The following are the features of an ideal ABE:

- **Data Confidentiality:**Unauthorized users are unable to read the plain text of the data, which means that they are unable to learn about the encrypted data. In this situation, the unauthorised user lacks sufficient attributes to meet the access policy's requirements. Unauthorized access to the plain text of the encrypted data from KGC and the data storage centre should be avoided as a result.

- **Collusion Resistance:**The dishonest user can decipher encrypted data by combining their attributes. Collusion resistance is one of the most important security aspects for ABE systems. Even if none of the users can decipher the ciphertext

individually, combining their attributes may allow them to decode it.

- **User/Attribute revocation:**People who leave the system can have their access rights revoked by the schemes.

A. *Attack Analysis*

Cryptography is a difficult undertaking that aims to make data unintelligible without knowing a secret key (Asymmetric cryptography uses private key where Symmetric cryptographyuses a shared key) [34].Fig. 26 represents the types of Attacks in Cryptographic system.

Types of Attack in Cryptography

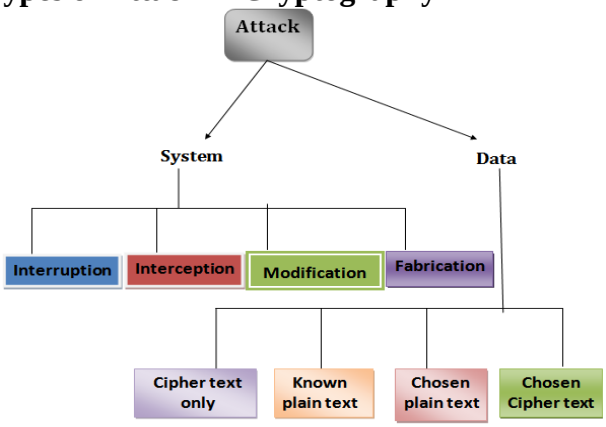


Fig. 26. Types Of Attacks Diagram

B. *System Attacks*

- In general, data flows from source to destination. System assaults are those that target the flow of information. Fig. 27 depicts System Attack.

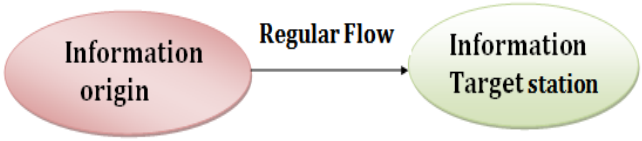


Fig. 27. System Attack

a) Interruption: It's an attack on the resource's availability. When data going from the source to the destination becomes useless or unavailable. Fig. 28 express the Interruption process in System Attack.

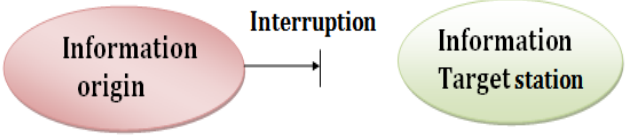


Fig. 28. Interruption diagram

b) Interception: It's a breach of system security. A trusted party has access to the model in this attack. Unauthorized parties can be people, programmes, or computers. Fig. 29 indicates about how Interception attack occurs.

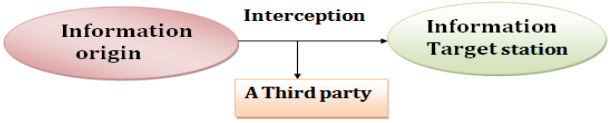


Fig. 29. Interception diagram

- *Modification:* It is a breach of the system's integrity. In this assault, an unauthorised party has not only access to the asset, but also the ability to modify it. Fig. 30 shows the generation of Modification attack .

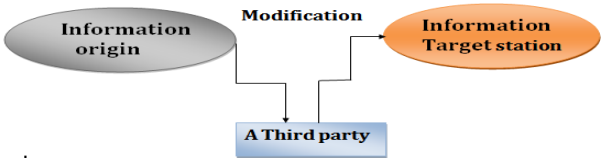


Fig. 30. Modification diagram

c) Fabrication: It's a smear campaign against the system's integrity. In it, an unauthorised entity enters the system and inserts counterfeit things. Fig. 31 describes about Fabrication process.

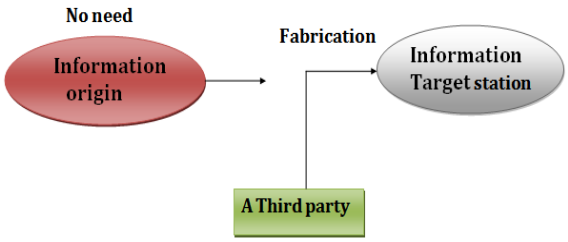


Fig.31. Fabrication diagram

XXI. DATA ATTACKS

An attack is a method of attempting crypto analysis. The amount of information that a

decoder can extract from a crypto system can be classified into four types of decryption:

A. ***Cipher text only attack*:**The crypto analyst use the same algorithm for encrypting of ciphertext of multiple messages. The plaintext or encryption key used in the messages must then be recovered. So then the encrypted messages can be deciphered using the same keys.If the key domain is tiny, a brute-force attack is viable. We have made the key size limitless because it's used to calculate each PRNG state 'Si' in $mod\ n$. As a result n needs to be big enough to handle huge keys.

B. ***Known plain text attack*:**Crypto analysts are eager for a profession that allows them to preserve the key or method used to encrypt or decrypt the messages [35].If an opponent only has access to a piece of plaintext-ciphertext pair, user could only derive the value of keys used to encrypt the plaintext. There is no information on how to produce successive streams of keys due to the value of K is required to calculate the next PRING state. Additionally if the same key is used to encrypt two plaintext values, the seed value will be different, resulting in a separate key stream.

C. ***Chosen plain text attack:***The crypto analyst has access to both the cipher and plaintext. An intruder has been identified and will be stationed at the encryption location inorder to carryout the attack. A selected plaintext attack is a form of cryptanalysis attack in which the attacker can encrypt arbitrary plaintext and obtain matching ciphertext[36]. The assault's purpose is to acquire more data in order to compromise the encryption system's security. A carefully designed plaintext assault in the worst case scenario could reveal the system's secret key. Plaintext injection attacks are a sort of selected plaintext attack in which the attacker injects a tiny chunk of plaintext.

Chosen plaintext attacks can be classified into two categories:

- A batch plaintext attack, in which the cryptanalyst selects all plaintext before encrypting any. When the term "selected plaintext attack" is used without qualifier, this is frequently the implication.
- Adaptive selected plaintext attack, in which the cryptanalyst selects consecutive plaintext depending on knowledge from prior encryptions through a series of interactive queries.

D. ***Chosen cipher text attack:*** In this case, the crypto analyst is in possession of the chosen cypher text as well as plain text that has been decrypted using the private key. It does, however, have access to an encryption machine. An attacker can use a decryption oracle to decipher any ciphertext in a targeted ciphertext attack. In most circumstances, the attacker must choose all ciphertext ahead of time before approaching the oracle. Rackoff and Simon(1991) formalized the adaptive chosen-ciphertext attack, allowing him to adjust his choice based on the oracle's interaction.

XII. SUMMARY

Security is very much needed in every aspects of life. For sharing files from one system to another security is concerned. Hence, in this paper, we have kept security as the pivotal part using cryptographic concepts.In this context, ABE scheme, KP-ABE and CP-ABE procedures have been discussed lucidly for secured data transmission. In this paper, many security attacks are clearly mentioned with their objectives and functions, those are quite helpful for future investigation in such fields. In the first part of our paper, we have covered basic concepts of cryptography along with its types in details. Afterwards, traditional cryptosystems with theirs functionalities are discussed with their cons. One of the most salient concept i.e. Public key cryptography is elaborated in this paper with its types. Furthermore, ABE, KP-ABE and CP-ABE schemes are explained individually with their working structure and comparisons. In addition, we have discussed various phases such as: key setup, key generation, encryption and decryption in each of the above written schemes separately which gives a clear understanding to a user for his future study in this field. RSA algorithm concept has also been clearly examined and discussed in our work , which will provide a better knowledge to the researcher who is interested to work in this field.

REFERENCES

[1] N. Sharma , Prabhjot and H. Kaur, "A Review of Information Security using Cryptography Technique," International Journal of

Advanced Research in Computer Science, vol. 8, pp. 323-326, 2017.

[2] A. Joseph Amalraj1, Dr. J. John Raybin Jose2 , " A Survey Paper On Cryptography Techniques", IJCSMC, Vol. 5, Issue. 8, pp. 55 – 59, 2016.

[3] A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," International Journal Of Engineering Development and Research, vol. 2, no. 2, pp. 1667-1672, 2014.

[4] SushreeBibhuprada B. Priyadarshini, Amiya BhusanBagjadab, Brojo Kishore Mishra,2018, Auerbach Publications, "Digital Signature and Its Pivotal Role in Affording Security Services", Pages20,eBook ISBN9780429468254.

[5] J. Chandrashekhara1 , Anu V B2 , Prabhavathi H3 , Ramya B R4, International Journal of Innovative Research in Computer Science & Technology (IJIRCST) , "A Comprehensive Study on Digital Signature" ISSN: 2347-5552, Vol. 9, pp. 43-47,2021 .

[6] G.Caire, E. Biglieri, "Linear block codes over cyclic groups" IEEE Transactions on Information Theory ,Vol. 41, Issue. 5, pp. 1246 – 1256,1995.

[7] M. Amara, A. Siad, "Elliptic Curves and their use in Cryptography", Signal Processing and their Applications, WOSSPA, IEEE, Tipaza, Algeria, May.

[8] K. Rabah ,"Security of the Cryptographic Protocols Based on Discrete Logarithm Problem", Journal of Applied Sciences, vol. 5,pp. 1692-1712, 2005.

[9] Jun Zhang, LiQunchen, "An Improved Algorithm For Discrete Logarithm Problem", International Conference on Environmental Science and Information Application Technology, IEEE, Wuhan, vol. 2, pp. 658-661 2009.

[10] Diffie, W. and M.E. Hellman, "New directions in cryptography", IEEE , vol. 22, pp. 644-654,1966.

[11] Okamoto, T., "Encryption and authentication schemes based on public-key systems", The University of Tokyo, 1988.

[12]Elgamal, T., "A public-key cryptosystem and a signature scheme based on discrete logarithms." IEEE Trans. Inform. Theory, vol. 4, pp. 469-472,1985.

[13] Shireen Nisha, Mohammed Farik, "RSA Public Key Cryptography Algorithm–A Review" International Journal Of Scientific & Technology Research Vol. 6 , pp. 187-191, 2017.

[14] Rohit Minni, Kaushal Sultania, Saurabh Mishra, Prof DuraiRaj , "An Algorithm to Enhance Security in RSA" , VIT University, IEEE – 31661,2018.

[15] QiangWang , Li Peng , Hu Xiong , And Zhiguang Qin, "Ciphertext-Policy Attribute-Based Encryption With Delegated Equality Test in Cloud Computing" IEEE,Vol. 6, pp. 760-771, 2017.

[16] R.M.Davis , "The data encryption standard in perspective", IEEE, vol. 16,pp. 5-9,1978 .

[17] Fahmi Ruziq1 , Poltak Sihombing2 , Sawaluddin2, "Combination Analysis of Data Encryption Standard (DES) Algorithm and LUC Algorithm on File Security", Vol.7, pp. 2454-2237,2020.

[18] "An overview of public key cryptography, M.E. Hellman, Department of Electrical Engineering, Stanford University, IEEE Communications Magazine ,vol. 40, pp. 42 – 49, 2002.

[19] M. Sandoval , M. Cabello1 , H. Marin-Castro, J. Gonzalez , "Attribute-Based Encryption Approach for Storage, Sharing and Retrieval of Encrypted Data in the Cloud",vol. 8, pp. 170101-170116,2020.

[20] H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, ''CP-ABSE: A ciphertext-policy attribute-based searchable encryption scheme,'' IEEE Access, vol. 7, pp. 5682–5694, 2019.

[21] Mr. Anup R. Nimje , Prof. V. T. Gaikwad ,Prof. H. N. Datir "Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview" International Journal of Computer Trends and Technology, Vol. 4, 2013.

[22] H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, ''CP-ABSE: A ciphertext-policy attribute-based searchable encryption scheme,'' IEEE Access, vol. 7, pp. 5682–5694, 2019.

[23] LyesTouati, YacineChallal, and AbdelmadjidBouabdallah,"C-cp-abe: Cooperative ciphertext policy attribute-based encryption for the internetof things",

2014 International Conference on, pp. 64–69. IEEE, 2014.

[24] J. Han, W. Susilo, Y. Mu, "Improving privacy and security in decen-tralized ciphertext-policy attribute-based encryption", IEEE Trans on Information Forensics and Security, vol. 10 (3), pp. 665–678,2015.

[25] V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data", Alexandria, Virginia, USA, 2006.

[26] R.Ostrovsky, A.Sahai, and B.Waters,"Attribute-based encryp-tion with non-monotonic access structures," , vol.19, pp. 195–203, 2007.

[27] Chang-Ji Wang, Jian-Fa Luo, "A Key-policy Attribute-based Encryption Scheme with Constant Size Ciphertext" Eighth International Conference on Computational Intelligence and Security,2012.

[28] JungyubLeea, Sungmin Oha , Ju Wook Janga, "A Work in Progress: Context based encryption scheme for Internet of Things" The 10th International Conference on Future Networks , pp. 271 – 275,2015.

[29] Kapadia, A., Tsang, P.P., Smith, S.W.: Attribute-based publishing with hidden credentials and hidden policies. In: Proc.Network& Distributed System Security Symposium (NDSS), pp. 179–192 ,2007.

[30] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," Cryptography and Coding: Cryptography and Coding 2001, LNCS, vol. 2260, pp. 360-363, 2001.

[31]Sahai and B. Waters. Fuzzy Identity Based Encryption. In Advances in Cryptology – Eurocrypt, vol. 3494, pages 457–473, 2005.

[32] Shenglong ,Yiming Zhao , Han Zhu, "Extending Fuzzy Identity-Based Encryption with Delegating Capabilities" IEEE,Vol. 1, pages 19 – 23, 2011

[33] Mustafa Mohammed Alhag, Yasir Abdelgadir Mohamed, "An Enhancement of Data Encryption Standards Algorithm (DES)"IEEE, 2018.

[34]Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya, "Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption"pp. 354–363 , 2004.

[35] Wenbo Shi ,Injoo Jang, "Chosen Ciphertext Secure Fuzzy Identity-Based Encryption Scheme with Short Ciphertext", IEEE, Seoul, School of Computer Science and Engineering, pp. 402-751, Korea, 2009.

[36] P. Louis Cayrel, Ousmane Ndiaye, "Critical attacks in code-based cryptography", International Journal of Information and Coding Theory , Vol. 3 , pp.158–176, January 2015.