International Journal of Computational Intelligence in Control

SECURITY ISSUES IN BIG DATA ANALYTICS AND ITS SOLUTION BASED ON INTEGRATED CRYPTOGRAPHIC ALGORITHM

Mrs. P.Punithalakshmi [1], Dr. M.Rajakumar[2]
[1]Research Scholar, Jamal Mohamed College, Trichy.
(Affiliated to Bharathidasan University, Tiruchirappalli)
Email: punithamphil1981@gmail.com,
[2] Research Advisor, Assistant Professor, Jamal Mohamed College, Trichy.
(Affiliated to Bharathidasan University, Tiruchirappalli)
Email: easwar_2007@yahoo.com

Received: 15th September 2021
Revised: 12th October 2021
Accepted: 06th November 2021

Abstract: In the emergence world of the data communications is engaged large volume of data handled in secure manner was not easily. The vendors of the data provide the access for many users in many forms. All social media and digital applications maintain the data volumes are increased in day by day. So that applications needs more storage space and also a secure medium for data retrieval process. The big data environment is an emergence new trend in the current world today. There are many kind unstructured data stored in different medium. Especially for financial based organization must enable the full secure based data maintenance in digital media. Most of the organization using a trusted secure online money transaction portal, that are provide a high confidential secure in financial vendors. Every digital based transaction are gets the verification on every time the account access. It must generate a authentication and confidentiality proof of each transaction. In this manner to the verification time is very peculiar because the session time of transaction is cross the limit, that transaction was declined. This processing time is to calculate the user and account verification performing cryptographic encryption and decryption process. In this paper concentrate the key generation algorithm to provide the high and powerful security on the financial organization that are maintain the big data values on their servers. Also this paper focused on the data analytical process with additional security of key generation algorithm in AES technique in cryptography.

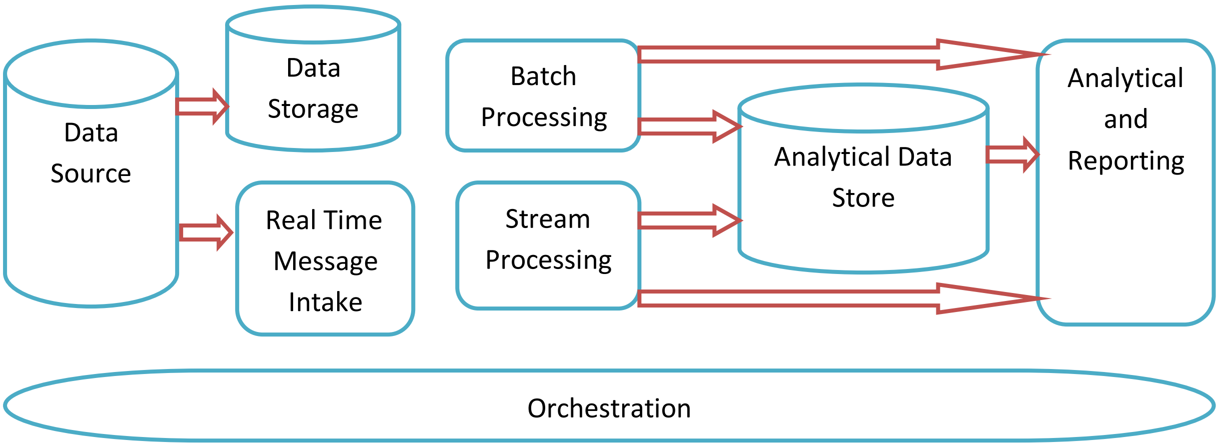
Keywords: Big data analytic, AES, ECDSA, ECC, Crime analysis, RC4 algorithm, KSA, PRGA.

I. INTRODUCTION

In the big data environment of the world are handling structured, semi-structured and unstructured data. It enables the 3V's data maintenance that is Volume of data, Verity of data, and Velocity of data. All users data, product information, agent service, medicine field related data, travels agencies data, satellite automation information, networks related data, electronic fund transaction on financial sector, etc., grew new pattern or model for maintain data by the concern organization. Data security is the challenging task for each organization that depends with many forms of security algorithm [16] [17] [18] [19] [20]. There are many type of data theft occurring in digital world by the hackers, intruders and some unauthenticated users. In this situation to provide security for the data as much as possible compared with before algorithms[21] [22][23].

1.1. Architecture and techniques of Big data:

This architecture is designed in such a way that it handles the ingestion process, processing of data and analysis of the data is done which is way too large or complex to handle the traditional database management systems. Different organizations have different thresholds for their organizations; some have it for a few hundred gigabytes while for others even some terabytes are not good enough a threshold value. Due to this event happening if you look at the commodity systems and the commodity storage the values and the cost of storage have reduced significantly. There is a huge variety of data that demands different ways to be catered. Some of them are batch related data that comes at a particular time and therefore the jobs are required to be scheduled in a similar fashion while some others belong to the streaming class where a real-time streaming pipeline has to be built to cater to all the requirements. All these challenges are solved by big data architecture.



a). Data Sources

The data sources involve all those golden sources from where the data extraction pipeline is built and therefore this can be said to be the starting point of the big data pipeline. The examples include:
(i) Data stores of applications such as the ones like relational databases

(ii) The files which are produced by a number of applications and are majorly a part of static file systems such as web-based server files generating logs.

(iii) IoT devices and other real time-based data sources.

b) Data Storage

This includes the data which is managed for the batch built operations and is stored in the file stores which are distributed in nature and are also capable of holding large volumes of different format backed big files. It is called the data lake. This generally forms the part where our Hadoop storage such as HDFS, Microsoft Azure, AWS, GCP storages are provided along with blob containers.

c) Batch Processing

All the data is segregated into different categories or chunks which makes use of long-running jobs used to filter and aggregate and also prepare data o processed state for analysis. These jobs usually make use of sources, process them and provide the output of the processed files to the new files. The batch processing is done in various ways by making use of Hive jobs or U-SQL based jobs or by making use of Sqoop or Pig along with the custom map reducer jobs which are generally written in any one of the Java or Scala or any other language such as Python.

d) Real Time-Based Message Ingestion

This includes, in contrast with the batch processing, all those real-time streaming systems which cater to the data being generated sequentially and in a fixed pattern. This is often a simple data mart or store responsible for all the incoming messages which are dropped inside the folder necessarily used for data processing [24] [25] [26] [27] [28][29]. There are, however, majority of solutions that require the need of a message-based ingestion store which acts as a message buffer and also supports the scale based processing, provides a comparatively reliable delivery along with other messaging queuing semantics. The options include those like Apache Kafka, Apache Flume, Event hubs from Azure, etc.

e) Stream Processing

There is a slight difference between the real-time message ingestion and stream processing. The former takes into consideration the ingested data which is collected at first and then is used as a publish-subscribe kind of a tool. Stream processing, on the other hand, is used to handle all that streaming data which is occurring in windows or streams and then writes the data to the output sink. This includes Apache Spark, Apache Flink, Storm, etc.

f) Analytics-Based Data store

This is the data store that is used for analytical purposes and therefore the already processed data is then queried and analyzed by using analytics tools that can correspond to the BI solutions. The data can also be presented with the help of a No SQL data warehouse technology like HBase or any interactive use of hive database which can provide the metadata abstraction in the data store. Tools include Hive, Spark SQL, Hbase, etc.

g) Reporting and Analysis

The insights have to be generated on the processed data and that is effectively done by the reporting and analysis tools which makes use of their embedded technology and solution to generate useful graphs, analysis, and insights helpful to the businesses. Tools include Cognos, Hyperion, etc.

h) Orchestration

Big data-based solutions consist of data related operations that are repetitive in nature and are also encapsulated in the workflows which can transform the source data and also move data across sources as well as sinks and load in stores and push into analytical units. Examples include Sqoop, oozie, data factory, etc.

II. REVIEW OF LITERATURE FOR EMERGENCE OF BIG DATA IN CRIME ANALYSIS:

Criminal activity is a worldwide common problem. Over the time, Crime incidents are increasing drastically and it is a significant threat for our society. Criminal are pretty smarter than crime investigation agencies (police department) with the help of new technologies. As per the statistics in India, A total of 95 Lakh crimes were reported in 2016 [9][8]. Criminal activities can be caused from several reasons. It is quite difficult to manage and investigate the incidents by agencies either due to lack of head counts of cops or criminals are more proactive. They are finding new way of doing it every day. Traditional method of monitoring and investigation for police department takes longer time to predict about the criminal profiles, to suspect the next future crime location, or to know the pattern of crime. The Big data analytics helps businesses analyze and examine large amount of data. The process involves hidden patterns, correlations and provides deep business insights to make an appropriate business decision. Basically, organizations have realized the strengths of big data analytics and its features. Businesses want to be more objective and data-driven and so they are embracing the power of data and technology. In the government and public sector, big data analytics as a major tool for data and forecasting analysis. Organizations have invested in big data analytics and are expected to make quick and agile business decisions to remain competitive. Here with to provide an impact for high security at the time of transaction was the biggest objective of thesis.

Most of banking system and finance related organizations face the important aspect in security issue for maintaining user data and transaction. They need very secure environment for handling information digitally and globally. All the organizations are spending money to protect their company information on a server. They use many kinds of cryptosystem procedure for store and retrieve data on server[6][8]. Protection of information the bank is a complex problem that cannot be solved only through the banking programs. Effective protection starts with selection and configuration of the operating system and network system [1]that support the functions of the banking program. Physical protection of various kind of mechanical, electrical and electro- mechanical devices and structure specially designed to create physical barriers on the possible way of information system and protected information. In banking sectors play a huge role in the economic life of society[7]. Theoretically, the legal framework for protection of banking information exists in our country, but it is far from perfect, while there were cases when the bank was punished for the disclosure of information.

In this paper the cyber crime over the social media using the data mining algorithms and compare the algorithm based of F-measure[2] value corresponding to the accuracy and the precision rate. Every social site collect user profile which contain personal information about user. These platform facilitate content sharing and increasing number of friends, viewing contents and so on. Random forest algorithm that calculate F-Measure factor used to compare the algorithm details.

$$F - measure = \frac{2 \times p \times r}{p + r}$$

Here p means Precision, r means Recall and F provide both that how robust the algorithm and level of accuracy of the classification.

Globally, cyber crime was the second most reported crime in the year 2016. In Yahoo company revealed that in the year 2013 over a billion accounts were hacked, and in the year 2015 another 500 million accounts were compromised. A Saudi hacker released 400,000 credit card information which was hacked from an Israeli sports website. In the year 2016 it was estimated that 3.2 million debit card were compromised in major Indian banks including SBI, HDFC, ICICI, Axis Bank etc. In September 2012, IEEE was exposed by its user names and plain text passwords for almost 100,000 of its members.

III. PROBLEM DEFINITION FOR SECURITY INFINANCIAL TRANSACTION

In financial sectors has promotes the facility for the users, there are many ways to transact the money from one to another with safe and authentication access. Each financial sector has maintained the separate application and website to manage this transaction. An important factor for this to unique identification for the customers or users, there exact contact number depends with each account. Any kind of money transaction[4] an auto generated OTP reach send to respective user contact number with maintain in bank account in particular financial sector. That OTP has the 3 minutes or 1 minute validity period at the time of transaction process. A security mechanism applied to this transaction with encrypted of MD5(Message Digest 5) hash function. Entire transaction handle with AES(Advanced Encryption Standard), RSA RC4that are making the transaction possible to encrypt even large bulk data transfers with minimal performance consequences.

In e-banking system are established in different way like ATM, Card, and Mobile banking system. ATMs were encrypted with DES, but the transaction processor requires the use of more secure triple DES. There were some smart intruders make fraudulent in ATM withdrawal, so AES algorithms uses security standard add support for CBC(Cyber Block Chaining) mode to IP Security(IPSec). In card type of transaction all the data and communications are protected using making chip and PIN. The EVM smart chip where EVM stands for Europay, MasterCard and Visa, the three companies that created this microchip authentication system for credit, debit and ATM cards is the small chip embossed on card.

IV. PROPOSED WORK FOR ENHANCING SECURITY

4.1. Implementation of enhanced RC4 algorithm

In RC4[3] algorithm is a symmetric stream cipher and variable key length. This symmetric key algorithm is used identically for encryption and decryption process. Here the data stream is XO Red with the generated key sequence. An proposed methodology of enhanced RC4 with Asymmetric key algorithm used and it is serial as it requires successive exchanges of state entries based on the key sequence. There are two phases of algorithm work with key generation.

An enhanced RC4 uses asymmetric key that is public key encryption, which is comparatively more secure form symmetric key system. It has pairs of keys are used to encryption and decryption process. All the financial sector uses as fixed mobile number for each customer of the banking process. In Public key crypto system prove the confidentiality and user authentication as an improved manner of customer unique identity.

For understanding the cybercrime prevention, asymmetric encryption and decryption process was made a secure transaction process. Because of the primary advantage of this process is that no need to securely transmit a secret key. Instead the public key is published openly, made available to the entire world. There is no need to keep it secret because it cannot be used alone. Asymmetric key encryption process work as like as follows.

1. The sender of a message uses the intended recipient's public key, which is freely available, to encrypt a message.
2. The recipient decrypts the message using his or her private key. Only the private key associated with the public key that encrypted it can be used to decrypt the message.

Ordinary Symmetric key encryption algorithm uses the following manner of key generation process for encryption and decryption.

a) Key Scheduling Algorithm(KSA) Phase:

- ✓ It is used to generate a State array by applying a permutation using a variable-length key consisting of 0 to 255 bytes.
- ✓ The state vector is identified as S[0], S[1].... S[255] is initialized with {0, 1, 2, ..., 255}. The key K[0], K[1], ..., K[255] can be of any length from 0 to 256 bytes and is used to initialize permutation S. E+ach K[I] and S[I] is a byte. Here I refer index of key element.
- ✓ K is a temporary array if the length of the key is 256 bytes copy it to K else after copying the remaining positions of K are filled with repeated Key Values until full.

```
          S[] is permutation of 0, 1, ..., 255
          K[] contains N bytes of key
fori = 0 to 255
  S[i] = i
  K[i] = key[i (mod N)]
i++
j = 0
fori = 0 to 255
  j = (j + S[i] + K[i]) mod 256
swap(S[i], S[j])
i = j = 0
```

b) Pseudo-Random Generation Algorithm (PRGA) Phase:

It used to generate keystream byte from State vector array after one more round of permutation.

```
Keystream Generation(i := 0, j := 0 )
while Generating Output:
i = (i + 1) mod 256
  j = (j + S[i]) mod 256
swap(S[i], S[j])
```

t = (S[i] + S[j]) mod 256

keystream Byte = S[t]

At each iteration, swap elements in table and select key stream byte. Then, perform XOR between the keystream generated and the plain text for encryption. Follow the same procedure as above for decryption, taking cipher text in place of plain text everywhere.

c) ECDSA process for improve the security in key generation process:

A recent technique for **ECDSA** provides the security in enhanced way for high sensitive digital based money transaction. Many countries are used this key security mechanism for bit coins and liquid fund related data security. In this paper have proposed methodology for ECDSA algorithm in online mode financial organization, are required more securing the customers data and banking information that are stored in database server. The process of this algorithm has the following steps.

- Elliptic curve digital signature algorithm is the elliptic curve analogue of DSA.
- ECDSA was first proposed in 1992 by scott van stone in response of NIST(National Institute of standards and technology),request for public comments on their first proposal for DSS. It was accepted in 1998 as an ISO standard, accepted in 1999 as an ANSI standard, accepted in 2000 as an IEEE standard.

➔Finite Fields:

Finite field consists of a finite set of elements F together with two binary operations of F called addition and multiplication that satisfied certain arithmetic properties.

The finite field of order q if and only if q is a prime power, then there is essentially only one field of order q, this field is denoted by F_p.

⇨ The finite field F_p

Let p be a prime number the finite field F_p called a prime field is comprised of the set of integers(0,1,2...p-1) with following arithmetic operations.

➔ Addition:

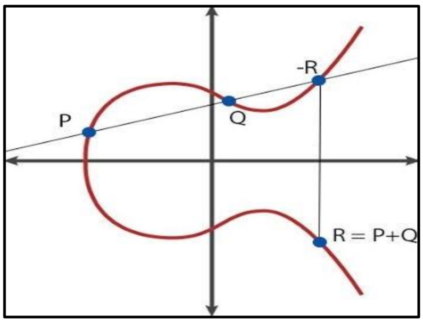


Figure.1. Elliptic curve points Addition

If a,b € F_p Then a+b=r where r is the remainder when a+b is divided by p and $0 \le r \le p\text{-}1$.

➔ Multiplication:

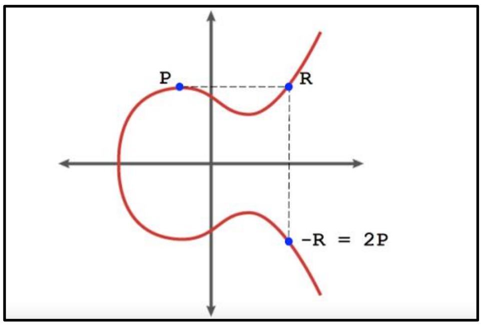


Figure.2.Ellliptice curve point Multiplication

If a,b € F_p then a-b=s ,where s is the remainder when a-b is divided by p and 0 ≤ s ≤ p-1.

➔ Inversion:

If a is a non-zero elements in F_P, the inverse of a modulo p denoted a^{-1} is a unique integer c € F_p for which a.c =1.

⇨ The finite field F_2m:
The field F_2m, called a characteristic two finite field or a binary finite field, can be viewed as a vectors space of dimension m over the field F_2 , which consist of the tow elements 0 and 1. That is there exist m elements $\alpha_1,\alpha_2,\alpha_3,\ldots\alpha_{m-1}$ in F_2m such that each elements α € F_2m can be uniquely written in the form,

$$\alpha = a_0\ \alpha_0 + a_1\ \alpha_1 + a_2\ \alpha_2 + \ldots + a_{m-1}\ \alpha_{m-1}\text{, where } a_i \text{ € } F_2m$$

d) Proposed Key Generation in Asymmetric key Generation:

An proposed asymmetric key encryption and decryption process uses in this research work with support of Elliptic Curve Digital Signature Algorithm(ECDSA) that was derived from Digital Signature Algorithm(DSA). ECDSA is also used for Transport Layer Security(TSL), and Secure Sockets Layer(SSL), by encrypting connection between web browser and a web application. The encrypted connection of HTTPS website, is made through signed certificates using ECDSA. The main feature of ECDSA versus RSA, is that ECDSA provide a higher degree of security with shorter key lengths. The following Figure.3 denote the flow diagram for ECDSA signature verification process.

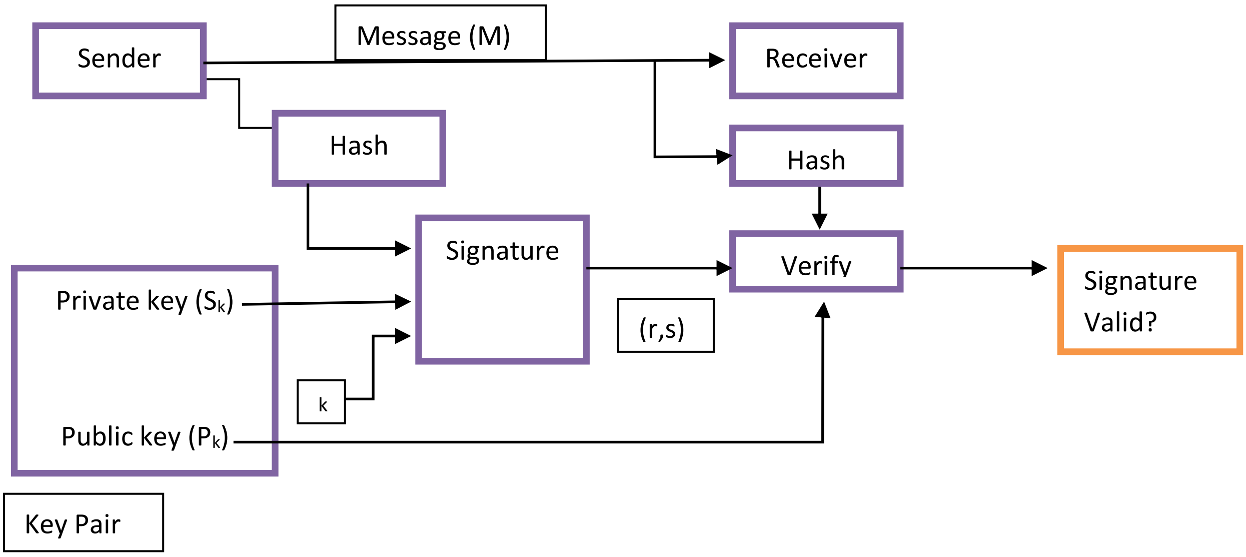


Figure:3. ECDSA Algorithm flow diagram.

In an digital signature algorithm, the original message are hash with AES technique and signed using the private key of sender and it sent to receiver. After the received encrypted message are decrypted using the hash message with public key of sender. The verification process are made on signed message, if the signature is valid the message are arrived as what the sender sent. Otherwise that message may be hacked and cracked by attackers. In this proposed technique for key generation process was more secure with high bit key of processing that are not able to identified by the cracker. This technique as follows,

Here, $r=k.G$

$s=k^{-1}(H(M)+r*s_k)$

Cipher text: $C=s^{-1}(\text{Mod } N)$

$u_1=H(M)*C(\text{Mod } N)$

$u_2=r*C(\text{Mod } N)$

Plain Text: $P=u_1*G + u2*P_k$, here prove $r==p(\text{Mod } N)$

Here, ECDSA signing and verification process has r and s are uniquely represent the signature. And z=(H(M)) is the hash of the message we want to sign.

1. Normally it required to use the left-most N bits of the hash, where N is the length of the hash function used. The hash algorithm turns an arbitrarily large amount of data into a fixed length hash. The length of hash function used SHA256, equals the bit length of the secp256k1 curve.
2. k is cryptographically secure random number which is used as a nonce to calculate the r and s values.
3. S_k and P_k these are the private key number and public key point respectively, used to sign and verify the message. Compressed public key are 33 bytes, consisting of prefix either 0×02 or 0×03 and a 256-bit integer called x. The uncompressed key are 65 bytes, consisting of constant prefix(0×04), followed by two 256-bit integers called x and y.
4. In signing algorithm compute the signature pair r and s from S_k and z. It generates a cryptographically secure random number k between 1 and n-1.

   $$\text{Compute}(x,y)= k * G,$$

   Where, G is the generator point of the secp256k1 curve, which is 04.

   Here, Compute r=x mod n. If r=0, generate another random k and start over.

   Compute $s=k^{-1}(z + r *S_k) \bmod n$. If s=0, generate another random k and start over.

5. In Verification algorithm ensure that the signature pair r and s, Q_A and z are all consistent.
   Verify both r and s are between 1and n-1.

   $$\text{Compute } u1= H(M)*C(\text{Mod } N)$$
   $$\text{And, compute } u2= r*C(\text{Mod } N)$$
   $$\text{Compute } (x,y) = u1* G + u2 * P_k$$

   And ensure it is not equal to the point at infinity.

   The point at infinity is a special point that results when you add two points whose result would otherwise not lie on the curve, such as two points with the same x value but inverted y values.

   If r=x mod n then the signature is valid. Otherwise, or if any of the check fail, then the signature is invalid.

e) Encryption and Decryption process:

In this research work focused on big data analytic with secure the data. This work of analysis based on multileaner and random forest algorithm suitable of best analytical result in financial sector data. Because of current trends in this world all the financial sectors operations are moving through digital money, liquid fund and bit coins range. Those things are basically depends with financial sectors and its applications. Those provide the authentication access and very essentially maintain the account in digitally. Also in large population areas, like Indian country handle each people personal information are stored in separate high end servers. Here whenever it needed, that data are processed with full of scope. Also multiple servers are maintains the data in cloud network servers and share the information with authentication and confidentiality.

In this proposed work of security system in this big data, provide high secure to access the information it may take some more seconds to take encryption and decryption process comparatively symmetric key system. But it take nearly 20 seconds for the process of encryption also give highly secure for to the data access at the time of money transaction.

f) Encryption process with Updated key generation mechanism:

Step 1: when entering on ATM service through money transaction, insert the card to machine or Enter account number into machine.

Step 2: Initially the transaction has to complete with PIN number for prove that authentication of customer.

Step 3: At the time of transaction in proposed system must prove the confidentiality and authentication.

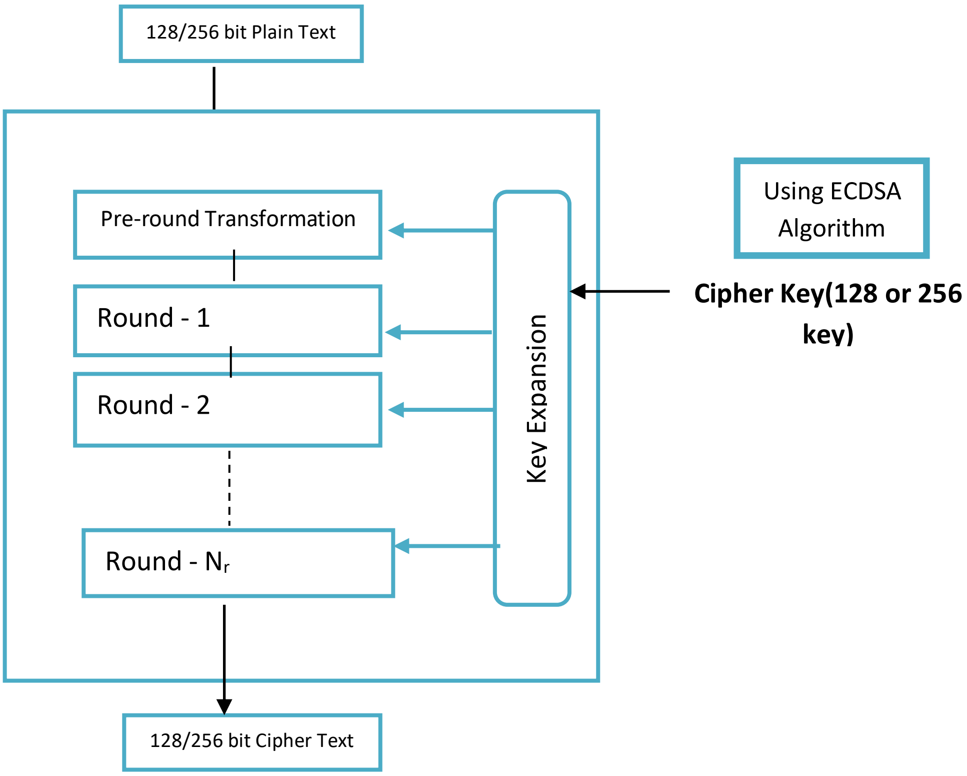


Figure.4.Flow diagram for AES algorithm

V. RESULT DISCUSSING

a) Sample process of working with ECDSA:

General form of Elliptic curve is $y^2=x^3+ax+b$

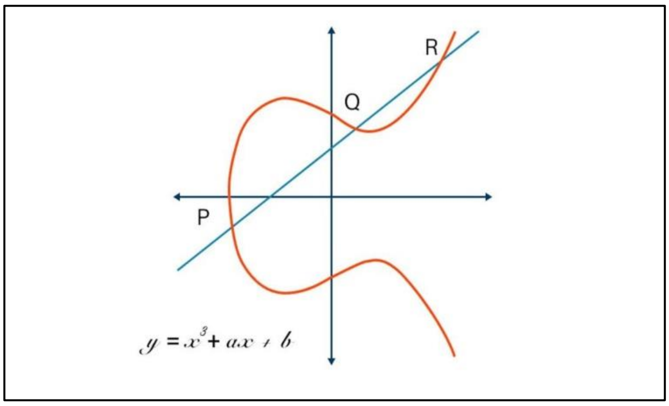


Figure.4. General form of elliptic curve for $y^2=x^3+ax+b$

Let , $E_{11}(1,6)$, here a=1, b=6 n=11

Ie, $y^2=x^3+x+6$ (mod 11)

from the above equation to find the (x,y) coordinate key points from the elliptic curve,

y	y^2 (mod 11)
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

x	x^2+x+6 (mod 11)
0	6
1	8
2	5
3	3
4	8
5	4
6	8
7	4
8	9
9	7
10	4

Table.1: find (x , y) coordinate point from Elliptic Curve.

Pick the (x,y) coordinate points from the above Table.1, for applying the Elliptic curve with user defined limitation (n) among the curve as (2,4),(2,7),(3,5),(3,6),(5,2),(5,9),(7,2),(7,4),(8,3),(8,8),(10,2) and (10,9). Using this points need to find the elliptic curve addition and multiplication for generate secret key.

Here P+Q is the mirror point of the elliptical curve with limitation point n, to fine (x_3,y_3) point using,

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right).(x_1 - x_3)$$

Let consider, $y^2= x^3 + ax+b$ $(GeneralForm)$
Take $y^2= x^3- 36$ & a=-36, b=0
Here, let's take: P = (-3, 9), Q = (-2, 8)

$$x_3 = \left(\frac{8-9}{-2+3}\right)^2 - (-3) - (-2)$$

$$= (-1)^2 + 3 + 2 = 1 + 3 + 2 = 6$$

$$y_3 = -9 + \left(\frac{8-9}{-2+3}\right)(-3-6)$$

$$= -9 - 1(-9)$$

$$= -9 + 9$$

$$= 0$$

$$\therefore \mathbf{P + Q = (6, 0)}$$

For find 2P using,

$$x_{3=}\left(\frac{3(-3)^2 \quad + (-36)}{2.9}\right)^2 - 2(-3)$$

$$= \left(\frac{27 + (-36)}{18}\right)^2 + 6$$

$$= \left(\frac{27 - 36}{18}\right)^2 + 6$$

$$= \left(\frac{-9}{18}\right)^2 + 6$$

$$= \left(\frac{-1}{2}\right)^2 + 6$$

$$= \frac{1}{4} + 6$$

$$x_3 = \frac{25}{4}$$

$$y_3 = -9 + \left(\frac{3.9-36}{18}\right)\left(-3 - \frac{25}{4}\right)$$

$$= -9 + \left(\frac{-9}{18}\right) . \left(\frac{-37}{4}\right)$$
$$= -9 + \frac{37}{8} = \frac{-35}{8}$$

$$\mathbf{2p = \left(\frac{25}{4} , \quad \frac{35}{8}\right)}$$

b) **Elliptic curve cryptosystem:**

Let consider the elliptic curve, as $y^2= x^3 + ax+b$, and Elliptic point with respect to one incident point as $E_p(a,b)$, then,

$$Q=k.P \text{ where } k<n , \qquad \text{(n is limitation)}$$

Here k is difficult to find to hackers because of using Discrete Logarithm problem of elliptic curve. Key exchange mechanism for ECC was done using the following. Let consider $E_q(a,b)$, this is elliptic curve with parameter a,b and q is a prime number, it is an integer values of form $2^{m.}$ G is point of elliptic curve whose order is very large value of n.

User A key Generation:

Select private key $n_{A;}\ n_{A<}n$

Calculate public key P_A ; $P_{A=}n_{A.}G$

User B key Generation:

Select private key $n_{B;}\ n_{B<}n$

Calculate public key P_B ; $P_{B=}n_{B.}G$

Calculate secret key of User A is, k= $n_{A.}\ P_{B.}$

Calculate secret key of User B is, k= $n_{B.}\ P_A$

Elliptic Curve Cryptography Encryption:

Here M- is Message, then encode M point on the EC, P_m , for encryption choose a positive random integer value k.

Cipher point $C_M=\{k.G, P_M+k.P_B\}$

Elliptic Curve Cryptography Decryption:

Setp-1: by receive the private key, $k.G.n_B$

Setp-2: $=P_M+k.P_B - k.G.n_B$

$=P_M+k.n_B.G - k.G.n_B$ ie. $P_B=n_B.G$

$=P_M$

VI. Result and Discussion and Comparison

In this work of asymmetric key system provide the high security on the transaction. Normally an asymmetric key system takes more seconds of processing time comparable with symmetric key system. But it provides high security on the transaction processing. In particularly for financial transaction, all the financial related or banking related online money transfer or ATM transaction, Debit card and Credit card related transaction. Mainly to focus this research work based on credit card fraud transaction, this process of updated security mechanism applied for the finance related transaction are get high secure encryption password to maintain the account. So possibility of the hacker try to hack an account is exceedingly difficult. ECDSA keys and signatures are shorter than in RSA for the same security level. A 256-bit ECDSA signature has the same security strength like 3072-bit RSA signature. The table 2 denote the key generation processing time of Symmetric and public key cryptosystem. Here to receive the optimum time for key generation process and produce the efficient and more secure key for encryption and decryption work of AES algorithm.

Key generation(bit)	Symmetric key System (Processing time)	Asymmetric key System (Processing time)
128 bit key input	25seconds	20seconds
256 bit key input	33seconds	28seconds

Table.2: Comparison for different key system

ECC's smaller key size is 256 as shown below Table 3. It is more efficient than RSA and it is more suitable for resource in net banking or other online based transactions. The basic idea of ECC is the general assumption that the elliptic curve discrete logarithm problem is infeasible or at least not solvable in a reasonable time.

RSA Key	Elliptic Curve Key
1024	160
2048	224
3072	256
7680	384
15,360	521

Table.3: Strength of ECC key in Proposed system

KEY LENGTH(BITS)		TIME (SECS)	
ECC	RSA	ECC	RSA
163	1024	0.08	0.16
233	2240	0.18	0.47

Table.4. Key generation time different for RSA and ECC

KEY LENGTH(BITS)		TIME (SECS)	
ECC	RSA	ECC	RSA
163	1024	0.15	0.01
233	2240	0.34	0.15

Table.5. Signature generation time different for RSA and ECC

KEY LENGTH(BITS)		TIME (SECS)	
ECC	RSA	ECC	RSA
163	1024	0.23	0.01
233	2240	0.51	0.01

Table 6. Signature verification time different for RSA and ECC

The main benefit of ECDSA include the smaller key sixe that achieve the same security, making it useful when being implemented in hardware and the hardness of breaking other existing system. In this paper of our research work focused on high security in financial transaction were done by using above mechanism of ECC key generation with update of public key cryptosystem. The above result Table.4 key generation of RSA and ECC algorithm are comparatively 0.47 seconds for RSA provide same security of optimum second 0.18 seconds for ECC. Also in Table.5shows the optimum signature generation time comparatively ECC is better than RSA. Here same minimum bit range of ECC give high secures then high bit of RSA algorithm as well as the signature verification time for ECC is higher than RSA because of high secure key generation in ECC. On the Table-6 shows the signature comparison time it is optimum level using ECC algorithm. But it is optimum level of security in financial transaction and produces more secure transaction. The above result are done by our research work public key crypto system in using ECC key generation algorithm is better then RSA key generation.

VII. FUTURE ENHANCEMENT

In this research work focused on the security in online money transactions and financial based organization are to handle customer data of confidential information in secure manner from their database. In the recent survey of online transaction are developed through high secure provisions provided by the organization. Focused on the research work of more enhancing technique are used in our organizations, that are unable to access by the crackers and hackers the data should be more secure comparable from current mechanism. The future enhancement of the paper may apply high end data transaction like banking sectors are maintain the data are digital in high secure and optimise the problems loss of money through digital mode. It will reduced the crime rate of online transaction for financial organization.

VIII. References

[1]. "Technologies of safety in the bank sphere from cyber attacks", Nyrkov Anatoliy P., Abramova Kristina V., Koroleva Elena A., Gaskarov Vagiz D., Sauchev Aleksandr V. Chair of Comprehensive Information Security. 978-1-5386-4340-2/18/$31.00 ©2018 IEEE.

[2]. "Detection of Cyber Crime on Social Media using Random Forest" , Twinkle Arora, Monika Sharma, Sunil Kumar Khatri, from Amity Institute of Information Technology, Amity University, Uttar Pradesh on 2nd International Conference on Power Energy, Environment and Intelligent control, October 18-19,2019.978-1-7193-5/19/$31.00,2019 IEEE.

[3] "Different data encryption methods used in secure Auto Teller Machine Transactions", Navneet Sharma, Vijay singh rathore in International Journal of Engineering and Advanced Technology. ISSN: 2249-8958, Volume-1, Issue-4, April 2021.

[4] "Enhanced Security for ATM machine with OTP and Facial recognition features" , Mohsin Karovaliya, Saifali Karedia, sharad Oza, Dr. D.R. Kalbande in International Conference on Advanced Computing Technologies and Applications-2015(Elsevier-open access article) 1877-0509.

[5] "Secure online Transction algorithm: Securing Online Transaction using Two-Factor Authentication", Joseph Gualdoni, Andrew Kurtz, Ilvamyzyri, Megan wheeler and Syed Rizvi at Complex Adaptive Systems conference with Theme: October 30 – November 1,2017(Elsevier) 1877-0509.

[6] "Crime Analysis and Prediction Using Big Data", Aarathi Srinivas Nadathur, Gayathri Narayanan, Indraja Ravichandaran, Srividhya. S Kalylvizhi.j Department of IT, SRM Institute of Science and Technology, in International Journal of pure and Applied Mathematics, Volume 119 No. 12, 2018,(207-211).

[7]. "Crime analysis using K-Means Clustering", Jothy agarwal, Renuka Nagpal, Rajni Sehgal from Amity University, Nodia, at International Journal of Computer Applications , Volume 83 – No.4, December 2021.

[8]. "Behavior Analysis and Crime Prediction using Big Data and Machine Learning" ,Pranay Jha, Raman Jha,
Ashok Sharma from International Journal of Recent Technology and Engineering(IJRTE), ISSN: 2277-3878, Volume 8, Issue 1 , May 2019.

[9] "Crime Statistics," data.gov.in. [Online]. Available: https://data.gov.in/dataset-group-name/crime-statistics. [Accessed: 07-May-2019].

[10].Johnson. Don and Menezes, Alfred."The Elliptic Curve Digital Signature Algorithm(ECDSA)",1999.
Web. http://cacr.uwaterloo.ca/techreports/1999/corr99-34.pdf.

[11].ANSI X9.31 Digital Signature using Reversible public key cryptography for the Financial services industry(rDSA),1988.

[12].I. Blake-G.Seroussi and N.Smart, Elliptic Curves in Cryptography, Cambridge University Press,1999.

[13].LAVANYA and V.NATARAJAN, " L wdsa: light-weight digital signature algorithm for wireless sensor networks"Sadhana,pp.1-15,2017.

[14].P. Longa and A. Miri, New composite operations and pre computation scheme for elliptic curve cryptosystems over prime fields(full version),"IACR Cryptology ePrint Archive,vol.2008.p.51,2008.

[15]. J. W, Bos, J, A, Halderman, N. Heninger, J. Moore M. Naehrig, and E. Wustrow, "Elliptic curve cryptography c2c communications focusing on security aspects," in Applied Machine Intelligence and Informatics(SAMI),2017 IEEE 15th international Symposium on, IEEE, 2017,pp.000461-000 466.

[16] Subhashini, M., & Gopinath, R., Mapreduce Methodology for Elliptical Curve Discrete Logarithmic Problems – Securing Telecom Networks, International Journal of Electrical Engineering and Technology, 11(9), 261-273 (2020).

[17] Upendran, V., & Gopinath, R., Feature Selection based on Multicriteria Decision Making for Intrusion Detection System, International Journal of Electrical Engineering and Technology, 11(5), 217-226 (2020).

[18] Upendran, V., & Gopinath, R., Optimization based Classification Technique for Intrusion Detection System, International Journal of Advanced Research in Engineering and Technology, 11(9), 1255-1262 (2020).

[19] Subhashini, M., & Gopinath, R., Employee Attrition Prediction in Industry using Machine Learning Techniques, International Journal of Advanced Research in Engineering and Technology, 11(12), 3329-3341 (2020).

[20] Rethinavalli, S., & Gopinath, R., Classification Approach based Sybil Node Detection in Mobile Ad Hoc Networks, International Journal of Advanced Research in Engineering and Technology, 11(12), 3348-3356 (2020).

[21] Rethinavalli, S., & Gopinath, R., Botnet Attack Detection in Internet of Things using Optimization Techniques, International Journal of Electrical Engineering and Technology, 11(10), 412-420 (2020).

[22] Priyadharshini, D., Poornappriya, T.S., & Gopinath, R., A fuzzy MCDM approach for measuring the business impact of employee selection, International Journal of Management (IJM), 11(7), 1769-1775 (2020).

[23] Poornappriya, T.S., Gopinath, R., Application of Machine Learning Techniques for Improving Learning Disabilities, International Journal of Electrical Engineering and Technology (IJEET), 11(10), 392-402 (2020).

[24]Karthikeyan, B., and Dr S. Hari Ganesh. "Encrypt-Security Improved Ad Hoc On Demand Distance Vector Routing Protocol (En-SIm AODV)." ARPN Journal of Engineering and Applied Sciences (ISSN: 1819-6608) 11.2 (2016): 1092-1096.

[25] Karthikeyan, B., N. Kanimozhi, and S. Hari Ganesh. "Analysis of reactive AODV routing protocol for MANET." 2014 World Congress on Computing and Communication Technologies. IEEE, 2014.

[26] Karthikeyan, B., Dr S. Hari Ganesh, and Dr JGR Sathiaseelan. "High Level Security with Optimal Time Bound Ad-Hoc On-demand Distance Vector Routing Protocol(HiLeSec-OpTiB AODV)." International Journal of Computer Science Engineering (E-ISSN: 2347-2693) 4.4 (2016): 156-164.

[27] Karthikeyan, B., N. Kanimozhi, and Dr S. Hari Ganesh. "Performance and analysis of ad-hoc network routing protocols in manet." NCAC (2013): 65-71.

[28] B. Karthikeyan, Detection of Selective Forwarding Attacks in Wireless Sensor Networks, International Journal of Electrical Engineering and Technology (IJEET), 11(9), 2020, pp. 376-392.

[29] B. Karthikeyan, Cluster based Malicious Node Detection for Mobile Ad Hoc Networks, International Journal of Advanced Research in Engineering and Technology (IJARET), 11(12), 2020, pp. 3501-3510.