A DELAY EFFICIENT PROTOCOL DESIGN FOR DATA COMMUNICATION

Safia K Muhammed
Department of Information Technology
Government Engineering College Painavu, Idukki
Email: safiakmuhammed@gmail.com
Sangeetha Jose
Department of Information Technology
Government Engineering College Painavu, Idukki
Email: sangeethajosem@gmail.com
Remesh Babu
Department of Information Technology
Government Engineering College Painavu, Idukki
Email: remeshbabu@yahoo.com

Abstract— Security and delay are the major issues in distributed system while storing or transferring of confidential data. Confidential or sensitive data can only accessed by authorized person. The users need to store their confidential data more securely within limited time. This paper propose a delay efficient protocol design for data communication with a novel algorithm implementation for protecting sensitive data stored in distributed system. The proposed algorithm is based on data masking techniques in which original data is masked with this algorithm and then encrypted with Advanced Encryption Standard (AES) algorithm. Here it uses two keys for data masking and encryption to provide high security. This paper also conducted a comparative study of three symmetric key encryption techniques which are AES, Data Encryption Standard (DES) and Triple DES (TDES).

Keywords— Data masking, AES, DES, TDES, Encryption Confidential data, Delay

I. Introduction (*Heading 1*)

Internet plays an important role in our daily life. Many new technologies are emerged such as cloud computing, internet of things etc based on internet Collection of autonomous systems which are connected through network and share resources is termed as distributed systems. Distributed systems mainly built up for sharing and storing of confidential data. Confidential data is nothing but the sensitive data which should be protected for privacy. Hence it is necessary to secure the confidential data from unauthorized access in distributed systems. The figure 1 shows an overview of distributed system.

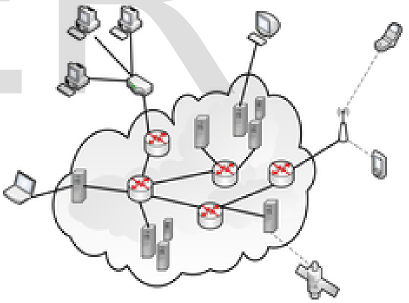
Fig.1 An overview of Distributed system

Cryptographic approach is an efficient way to protect the confidential data from unauthorized access. This approach can provide integrity, confidentiality, authenticity and access control to distributed systems. Cryptographic approach mainly divided into symmetric key cryptography [1] as well as asymmetric key cryptography. In a symmetric key cryptography, same key is used for encryption and decryption process. For example, if A and B want to communicate with a sensitive data, A encrypt the sensitive data (plain text) is encrypted using a secret key which is known by A and B. At the receiver side, B will decrypt the cipher text using the same secret key.

In asymmetric cryptosystem, two separate keys are used for encryption and decryption which are public key and private key respectively. For example, if C and D want to communicate each other then C encrypt data using D's public key then send to D. At the receiver side D decrypt the ciphertext using its own private key.

Symmetric key encryption consists of two type ciphers, block cipher and stream cipher. The block cipher further divide mainly Data Encryption Standard (DES), Triple Data Encryption Standard (T-DES) and Advanced Encryption Standard (AES). Example for stream cipher is RC4. Asymmetric key encryption consists of RSA, Diffie-Helman and DSA. Classification of cryptography shown in figure 2.

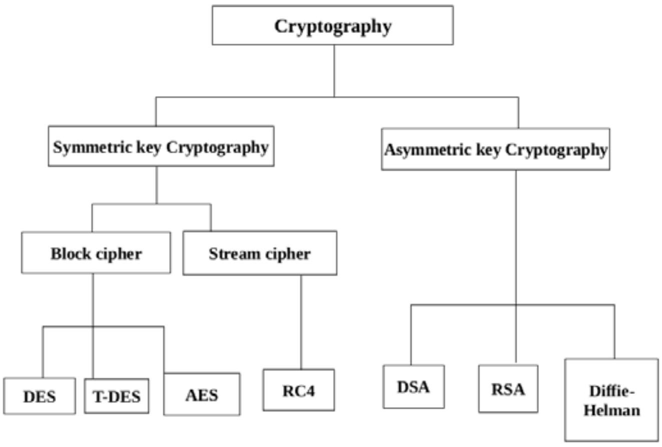

Fig. 2. Classification of encryption in cryptography

This proposed system uses an advanced encryption standard for securing confidential data since it have the following features:

- Security :- AES has resistance towards cryptanalysis attack as well as brute force attack.
- Cost :- It provides computational efficiency and storage requirement such as hardware, software or smart cards and also provides flexibility and simplicity.

AES provide 128 data block and key size is depending on number of rounds. If key size is 128 then number of rounds is 10. If key size is 192 then number of rounds is 12. If the key size 256 then number of rounds is 14.

A. Modes of operation in Block Cipher

Block and stream cipher algorithm operate in different modes [8] some of them are stated as:

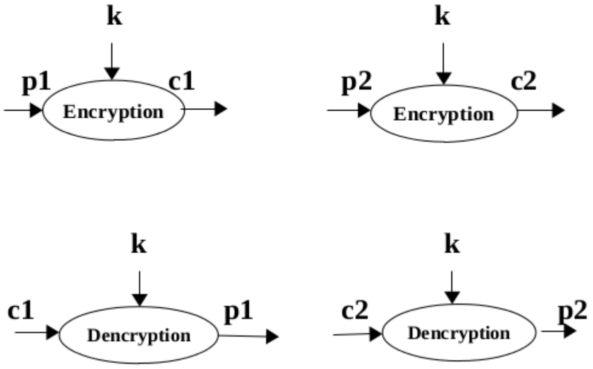

Fig.3. ECB mode operation for encryption and decryption

1) *Electronic code book mode (ECB)*: In the ECB mode operation, encrypt each block separately. There is impossibility for chaining process as well as error generation. When using ECB mode operation, the replay will easily capture the data which is a disadvantage. ECB mode operation for encryption and decryption shown in figure 3. In this figure, k is symmetric key, p1 and p2 are plaintext in each block and c1and c2 are cipher text in each block. It describes each plaintext block is encrypted using symmetric key and form ciphertext block. In the other side, it decrypt each ciphertext block using symmetric key and get plaintext blocks.

2) *Cipher block chaining (CBC)*: The main feature of CBC mode is the chaining mechanism in which each plaintext is depends upon preceding ciphertext block. Hence a bit of error in any block affects all other block. The first plaintext is *XORed* with initialization value. Then previous ciphertext is *XORed* with plaintext for encryption. The advantage of this operation is that *XORing* process hides the plaintext pattern. The first plaintext is *XORed* with an initial value and encrypt data block shown in figure 4.

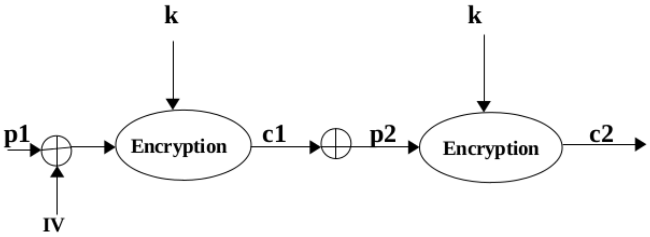

Fig.4. CBC mode operation in encryption

After the first operation, previous ciphertext XORed with next plaintext block so it is a chaining process. The decryption process is the reverse process of encryption that shown in figure 5.

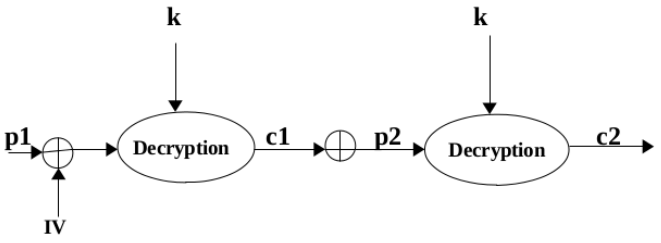

Fig.5. CBC mode operation in decryption

3) Cipher feedback: The chaining characteristics are similar to CBC mode. Besides that it also use initialization vector. Initialization vector does not need to be secret but it is different for each message.

4) Output feedback: It is similar to CFB in encryption with different block size. There is no chaining mechanism in this method. It also uses initialization value. Disadvantage is that plaintext can easily changed. This problem can overcome by using digital signature.

5) Counter: It does not depend on feedback mechanism. Initialization vector set at the sender and receiver side. Each plaintext is encrypted until last block. Decryption at receiver is the reverse process of encryption.

The rest of this paper is organized as follows:
Section 2 gives a literature survey and section 3 includes a comparative study of three symmetric key cryptography. Section 4 explains Data masking and its techniques. Section 5 provides proposed system design with proposed algorithm and AES technique. Section 6 explains case study of the proposed system and section 7 conducted result analysis. Final section concludes the work.

II. LITERATURE REVIEW

The paper [3] proposed perturbative masking techniques for data masking for preventing from unauthorized access. In this method, data transformation technique and bit transformation techniques are used. These techniques are used to protect sensitive numeric data in micro data table. The data transformation technique is better than bit transformation technique. Privacy preserving data mining is a novel research area in the field of data mining. It uses statistic disclosure control techniques for protecting sensitive data in a micro data table. Statistical disclosure control also known as inference control in statistical database. Tabular data protection brings out statistical aggregate information. It is an oldest method. The limitations of this system are it does not provide private information and there is no explicit individuals. Dynamic database do not gather information on specific individual. Microdata protection consists of n records and m attributes.

The paper [2] proposed a privacy application infrastructure for confidential data masking. This system provided two solutions. First one is to build an infrastructure to meet confidential information requirements and second one is to provide an application approach to mask confidential information. The sensitive data stored and processed by service taker. PIA deployed around the service taker. The major merits of this system are that it provides integrability, manageability and security. PIA privacy policy provides URL rewriting and skinning of HTML pages for white labelling. For storing sensitive data PIA database is used.

The paper [12] described the importance of cryptography in network security. Different types of cryptography are secret key, public key and hash function. In network security, problem exists in the area of secrecy, authentication, no reputation and integrity control. It explained the attack in cryptographic area which is known plaintext and cipher text only attacks, chosen plaintext and chosen ciphertext attack, adaptive chosen plaintext and adaptive chosen cipher text.

The paper [7] present calculations needed in the AES and RSA algorithm. It also described computational issues and different types of attacks and prevents data from this attack. This paper concluded from its analysis that RSA algorithm is complex than AES algorithm. AES is an efficient algorithm but have some issues in secret key exchange which can be solved by using RSA.
The paper [11] presents cryptographic approach and different types of cryptographic algorithms. They proposed an algorithm for encryption and decryption. This algorithm is very simple and reverse process performs high security. This algorithm is suitable for small amount of data. The paper [13] described overall view of encryption and decryption process in block ciphers. They proposed secure and flexible cryptographic mechanism. It is mainly used for a key management mechanism and it provide encryption secret key, shared secret key and decryption secret key which can help to prevent sensitive data.

The main goal of data masking is to protect sensitive data from outside world and [1] proposed a new approach for data masking by protecting sensitive data from unauthorized access. They also proposed four approaches that overcome limitations in traditional data mining . These four approaches are min-max normalization, fuzzy logic, rail-fence and map range. These approaches can generate masked data that can only accessed by intended user. The paper [5] addresses the problem of releasing microdata. The approach is based on the definition of k-anonymity. A table provides k-anonymity if attempts to link explicitly identifying information to its content map the information to at least k entities. They illustrate how k-anonymity can be provided without compromising the integrity (or truthfulness) of the information released by using generalization and suppression techniques. They introduce the concept of minimal generalization that captures the property of the release process not to distort the data more than needed to achieve k anonymity, and present an algorithm for the computation of such a generalization. They also discuss possible preference policies to choose among different minimal generalizations. The paper [9] report on the development of the Advanced Encryption Standard (AES).

III. COMPARATIVE STUDY

It compares three types of symmetric key encryption algorithm because these are popularly used. Three algorithms are Data Encryption Standard (DES), Triple Data Encryption Standard (T-DES) and Advanced Encryption Standard.

A. Data Encryption Standard (DES)

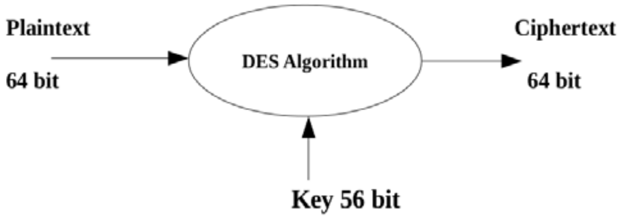

Fig.6. Overview of Data Encryption standard

Figure 6 shows the overview of DES. DES is a symmetric key algorithm used for encryption and decryption process. The block size in DES is 64 bits and key size is 56 bits. The extra eight bits are used as parity bits. In this algorithm 16 rounds are performed. In the working of DES, initial and final permutation is just reverse process and round function is an important part in DES. The 48 bits key applied to 32 bits input to give 32 bits output. Round key only applied when the two values are equal length hence the 32 bit data expanded to 48 bits then *XOR* with round key substitution box change to 32 bit output. In the key generation process, the initial stage of key size is 64 bits including parity bits. First step to drop parity bits and generate 56 bits key, these bits are split into two and shift left then generate first round key. Similarly, sixteen round keys are generated. The DES algorithm is complete and efficient but some of the selected keys are weak keys.

B. Triple DES

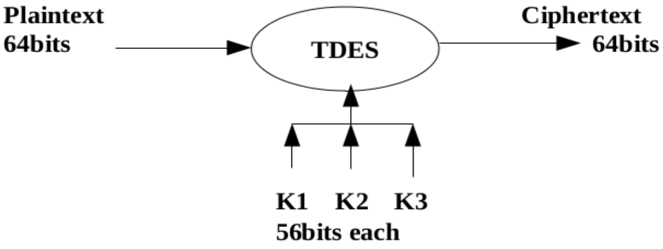

Fig.6. Overview of Data Encryption standard

TDES is also a symmetric block cipher and overview is shown in figure 7. Triple DES or 3DES is a symmetric key block cipher. It overcomes the limitations of DES. It consists of three different keys k1, k2 and k3. So the total key size is 168 bits. The working of TDES is first encrypt with k1 then decrypt with k2 and then encrypt with k3. Hence this process is called encrypt-decrypt-encrypt process. Here DES algorithm performs three times with different keys. If the k1, k2 and k3 are same value then perform DES operation. This algorithm more secure than DES but it has large delay since DES is performed three times.

C. Advanced Encryption Standard

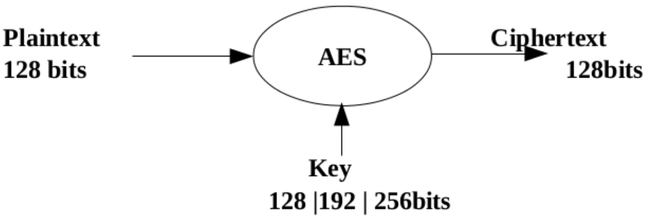

Fig.8. Overview of AES

AES is a symmetric block cipher and figure 8 shows overview. AES also a symmetric block cipher. It is a popularly used algorithm. It is six time faster than TDES. The block size is 128 bits and number of rounds depending on the key size .It provides high security. Same key is used for encryption and decryption. AES has different key size these are 128,192 and 256 bits for rounds 10, 12, 14 respectively. It is an efficient method for protecting sensitive data.

TABLE 1
COMPARISON BETWEEN AES, DES AND TDES

Properties	DES	T-DES	AES
Type	Symmetric key	symmetric key	symmetric key
Key size	56 bits	168 bits	128,192,256 bits
Block Size	64 bits	64 bits	128 bits
Rounds	16	48	10, 12,14
Speed	Slow	Very slow	High
Security	Very low	Moderate	High secure
Resource consumption	High	Moderate	Low

The table 1 describes comparison between AES, DES and TDES. The key size of DES is 56 bits long but TDES provide key size is 168 bits and AES provide different key length depending on number of rounds. So, AES mainly use three key sizes, these are 128 bits for round 10,192 bits for round 12, 256 bits provide for round 14.The data transferring through the networking block. The TDES and DES provide block size of 64 bits, but AES provides 128 bits. The speed of DES is slow because high computational complexity. TDES is very slow because three times DES is used. AES performs high speed because low computational complexity. DES provides very low security. TDES provide moderate security and AES provide high security. The resource consumption is high in DES, TDES has moderate and AES has low.

IV. Data Masking

Data masking is a method to hide data from unauthorized access. It provide security, mainly it is used in organizations for software testing and user training. The need of data masking is sometime does not require original data so data stored safely.

A. Data Masking techniques

Different types of data masking techniques for mask original data and these are explained below:

1) Substitution: It is an efficient method for applying data masking. It replaces original data with another data. Important thing is to mask the data for personal identifiable data, personal sensitive data or commercially sensitive data. This method can apply different data in database. It is not only protecting the data but also easily access by intended users.

2) Shuffling: Shuffling is a common method used for data hiding. It is similar to substitution method but it exchanges each character from original data. It is simple method to randomly shuffle data. If anyone has knowledge about original data then he can easily derived from masked data.

3) Number and Date Variance: In this method numeric value is used for masking the data and it is a useful method. If the variance is applied to number value then it provides meaningful data. The same thing is applied while using data variance.

4) Encryption: It is a complex method to solve the data masking issue. In this technique a key is applied to view original data. If key is revealed other than authorized person then the original data is accessed by those key holders. For encryption best method is AES algorithm.

5) Nulling Out/Truncating: It is a simplest approach and masking is performed while applying null value to data. It is only useful to prevent view of data. It maintain data integrity in masked data. It is fail in application logic validation.

6) Masking Out Data: Masking out is effective and simple method to prevent visibility of sensitive data. It is the extension of nulling out method because real data is keeping and not fully masked. This type of masking commonly used in ATM card, credit card etc. It is also known as dynamic data masking method. It is very useful method in billing system. Following are the limitations of the traditional data masking techniques:

- It is difficult to generate unique random values for each substitution.
- It is not effective while using less number of records.
- It is not well for numeric database.

V. SYSTEM DESIGN

The figure 9 shows the process of proposed system for protecting sensitive data using encryption along with masking technique. Sensitive data is a confidential data that can be accessed by intended users. In our system, this can be achieved by merging two entirely different techniques. That is data masking technique and AES technique. In the proposed data masking algorithm we can encapsulate data with some replacement. Then AES technique is used to encrypt masked data. This technique is very popular in cryptography because it provides accurate result with efficient delay.

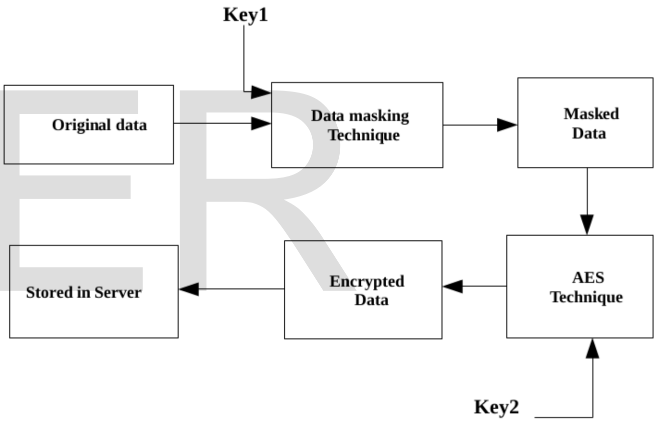

Fig.9. Process of proposed system using masking and encryption algorithm

The figure 10 describes the process unmasking and decryption in the proposed system. It is the reverse process of masking and encryption algorithm. If the intended user wants to retrieve data from server, AES technique with same key is used for decryption. Then the reverse process of masking technique applied on the decrypted data to unmask and retrieve the original data.

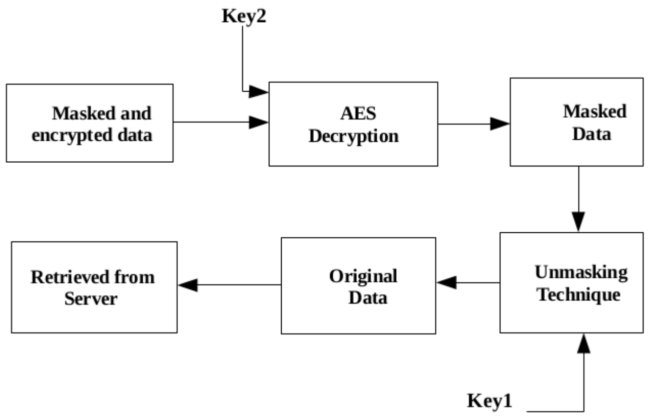

Fig.10. Process of proposed system with unmasking and decryption techniques

A. Hybrid AES and DM method

We propose new algorithm for protecting our confidential data by using hybrid AES and DM method. The algorithm 1 explains mask the data then encrypt by using AES method. These two are explained below:

```
input : Data D Random value R Key K
output: Encrypted masked data E
Start
C ← Length(D)
M ← square root (2* C)
Convert D to ASCII value
Represents ASCII value as matrix form (d[M][M])
for i ← 0 to m do
    for j ← 0 to m do
        a[i][j] ← d[i][j] + d[i][m]
        b[i][j] ← a[i][j] + R
    end
end
Reverse each value in matrix
Interchange lower and upper matrix elements
Diagonal element does not change
Encrypt data using AES with K
S ← E
Stop
```

Algorithm 1: Hybrid AES and DM method

B. AES algorithm

AES [8] is symmetric block cipher used to protect confidential data by applying encryption algorithm. It is widely used and most popular one. It is stronger and faster method because it perform faster computation. Its number of rounds depending on key size. i.e., 10 rounds for 128 bits key, 12 round for 192 bits key and 14 rounds for 256 bits key which is calculated from original AES key. In this algorithm, each rounds consists of four different process that shown in figure 11. The figure 11 show that flowchart of data encryption process using AES. The masked data as input and key is read from user interface. Then add round key depending on key size. We use key size of 128 bits; the round is set as 10. If the round does not reach 10, then perform and take sub bytes and shift rows then mix column values except in last round. Then add round and repeat until round reaches to ten repetitions. If number of round equal to ten then we get encrypted data.

- Byte substitution

The 16 byte input substituted to form a matrix with four rows and four columns.

- Shift rows

The four rows of matrix values are shifted to left. First row is not shifted. Second row shift one position, third row shifted two positions and fourth row shifted three positions. After this process we get a new matrix with 16 byte data.

- Mix columns

The matrix consists of four columns. These columns value transformed into new value by using mathematical operation. The input is four bytes to get output also four bytes with different values. This process does not applied on last column.

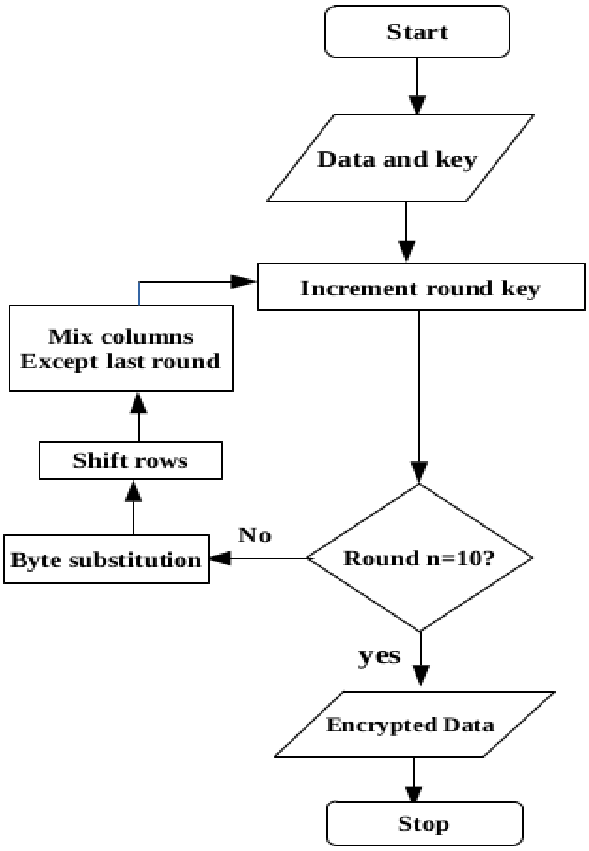

Fig.11. Data Encryption process using AES

C. Advantages of AES

- Secure

Because it is provide 128 bits data. If any brute force attack perform 2^128 attempt for accessing sensitive data. But it is does not possible.

- Faster

Less computational complexity of this algorithm performs high speed.

D. Disadvantages of AES

Key management is very weak by using this algorithm.

VI. CASE STUDY

Let “Hello” be the data that enter into the user interface and Perform proposed algorithm in stepwise as follows:
1) Start
2) Input the original data and calculate its data length. Since the data is hello and its length is five
3) If the length is equal to square of any number, then go to step 5. The data is not equal to square value then go to step 4.
4) Otherwise, padding is performed. We need data length of square of any number so we will padding some hash values. The data changed and length of the data is nine.
5) Convert to ASCII value represented as matrix form. Convert each character to ASCII form the values are 104,101,108, 108, 111, 42, 35, 35, 35 and represented as matrix form.

104	101	108
108	111	42
35	35	35

6) Each value added with last column value.
7) A key value added to this value and reverse it.

212 213 312 :: 0 0	209 210 012 :: 0 1	216 217 712 :: 0 2
150 151 151 :: 1 0	153 154 451 :: 1 1	84 85 58 :: 1 2
70 71 17 :: 2 0	70 71 17 :: 2 1	70 71 17 :: 2 2

8) Reversed values are represented as matrix form.

312	12	712
151	451	58
17	17	17

9) Lower and upper matrix are inter changed and diagonal element does not change.

312	151	17
12	451	17
712	58	17

10) These data encrypted using AES algorithm. The encrypted data is:
uOwtWmh5vNM6iooR9wArPWwDsFp4wBEtkow
7NWWJUEITVcpAgtRLP5H6SNI6m/7M

11) Encrypted data is stored in server. Decryption is just reversing the process of proposed method.

VII. RESULT ANALYSIS

This system mainly focused on security, hence proposed system used two algorithms to provide multilevel security. It has certain limitation related with memory. The figure 12 shows space complexity while encrypting original data. The storage space increases as the size of original data increases. The variation of execution time as the data size changes also analysed. The graph is given in table II. From the graph it is clear that the time increases as the size of data increases. Here compare DES, TDES and hybrid AES with DM method. We analysed that our system is efficient in delay. In a distributed system, it communicates like client server model. The user store the encrypted confidential data on server that can only accessed by that user and cannot be accessed by any unauthorized person and also the server. This system can be

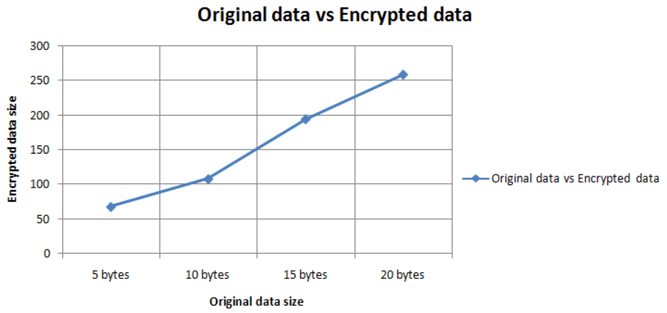

Fig.12. Storage space based on data size

TABLE II

EXECUTION TIME BASED ON DATA SIZE IN HYBRID AES WITH DM METHOD, DES AND TDES

Data size	Hybrid AES with DM method (µs)	DES (µs)	TDES (µs)
10 bytes	0.0013962	0.9008467	2.77025
20 bytes	0.0027923	1.8016934	5.05405
30 bytes	0.0041885	2.705421	8.31075
40 bytes	0.0055846	3.6033868	11.081
50 bytes	0.0069809	4.542335	13.85125
60 bytes	0.008377	5.40508	16.6215

used for securing confidential data like password, pin number etc securely stored on distributed systems. This system provides delay efficient encrypted data for sensitive data.

VIII. CONCLUSION

A delay efficient protocol is designed for data communication to provide high security in distributed system. We have studied the symmetric key encryption standards and data masking, we also compare different types of algorithms (AES, DES and TDES). Since AES provide better security and less implementation complexity, it has emerged one of the strongest and most efficient algorithms in existence today. It proposed a novel algorithm known as hybrid AES with DM method for masking the sensitive data. We used two separate keys for those two algorithms hence the attacker cannot access the confidential data.

References

[1] G. Sarada, N. Abitha, G. Manikandan, and N. Sairam, “A few new approaches for data masking,” in Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on, March 2015, pp.1–4.

[2] B. Liver and K. Tice, “Privacy application infrastructure: Confidential data masking,” in 2009 IEEE Conference on Commerce and Enterprise Computing, July 2009, pp. 324–332.

[3] S. Vijayarani and A. Tamilarasi, “An efficient masking technique for sensitive data protection,” in Recent Trends in Information Technology (ICRTIT), 2011 International Conference on, June 2011, pp. 1245–1249.

[4] “The security of confidential numerical data in databases,” Information Systems Research, vol. 13, no. 4, pp. 389–403, 2002. [Online]. Available: http://pubsonline.informs.org/doi/abs/10.1287/isre.13.4.389.74.

[5] P. Samarati, “Protecting respondents’ identities in microdata release,” IEEE Trans. on Knowl. and Data Eng., vol. 13, no. 6, pp. 1010–1027, Nov. 2001. [Online]. Available: http://dx.doi.org/10.1109/69.971193

[6] S. Vijayarani and D. A. Tamilarasi, “Bit transoformation perturbative masking technique for protecting sensitive information in privacy preserving data mining,” International Journal of Database Management systems (IJDMS), vol. 2, no. 4, 2010.

[7] A. A. Hasib and A. A. M. M. Haque, “A comparative study of the performance and security issues of aes and rsa cryptography,” in Convergence and Hybrid Information Technology, 2008. ICCIT ’08. Third International Conference on, vol. 2, Nov 2008, pp. 505–510.

[8] J. Daemen and V. Rijmen, The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.

[9] J. Nechvatal, E. Barker, L. Bassham, W. Burr, and M. Dworkin, “Report on the development of the advanced encryption standard (aes),” DTIC Document, Tech. Rep., 2000.

[10] W. Stallings, Cryptography and network security: principles and practices. Pearson Education India, 2006.

[11] M. Z. H. Sarker and M. S. Parvez, “A cost effective symmetric key cryptographic algorithm for small amount of data,” in 2005 Pakistan

[12] T. R. Devi, “Importance of cryptography in network security,” in Communication Systems and Network Technologies (CSNT), 2013 InternationalConference on, April 2013, pp. 462–467.

[13] A. M. AL-Abiachi, F. Ahmad, and K. Ruhana, “A competitive study of cryptography techniques over block cipher,” in Computer Modelling and Simulation (UKSim), 2011 UkSim 13th International Conference on, March 2011, pp. 415–419.