ENHANCEMENT OF SECURITY USING CRYPTOGRAPHIC TECHNIQUES

Natasha Saini[1] ,Nitin Pandey[2], Ajeet Pal Singh[3]

[1,2]*AIIT, Amity University , Noida ;* [3]*Raj Kumar Goel Institute Of Technology,Ghaziabad*

[1]natashamaniktahla@gmail.com,[2]npandeyg@gmail.com
[3]dr.ajeetpalsingh17@gmail.com

Abstract: The paper will describe various types of security issues which include confidentality,integrity and availability of data.There exists various threats to security issues traffic analysis,snooping,spoofing,denial of service attack etc. The asymmetric key encryption techniques may provide a higher level of security but compared to the symmetric key encryption Although we have existing techniques symmetric and assymetric key cryptography methods but there exists security concerns.A brief description of proposed framework is defined which uses the random combination of public and private keys.The mechanismsincludes:Integrity,Availabiity,Authentication, Nonrepudiation, Confidentiality and Access control which is achieved by private-private key model as the user is restricted both at sender and reciever end which is restricted in other models.A review of all these systems is described in this paper.

Keywords: **Plaintext,ciphertext , symmetric encryption, asymmetric encryption etc**

I. INTRODUCTION

The methodology of cryptography does not allow many people to actually understand the motivations in communication system. Cryptography methodology allows security at various level of network which focus on basic attributes of information security ie confidentiality,integrity and availability. The reason that lacks the security are efficiency, fault-tolerance and security[1].Public shared symmetric key is used in symmetric/secret method where a common key is shared between the encryption and decryption mechanism[2].Examples: DES,TDES,AES,Blowfish,RC4/RC5&Serpent.Encryption is used to convert plaintext to ciphertext and decryption is used to convert ciphertext to plaintext.However in assymetric or public key cryptography public key is used for encryption& private key is used for decryption and is efficient .RSA(Rivest,Shamir,Adleman)algorithm, ECC,DSA,ECDSA&DSS are the examples of public key cryptrography.

Diagrammatic Representation of Symmetric/Secret Key Cryptography

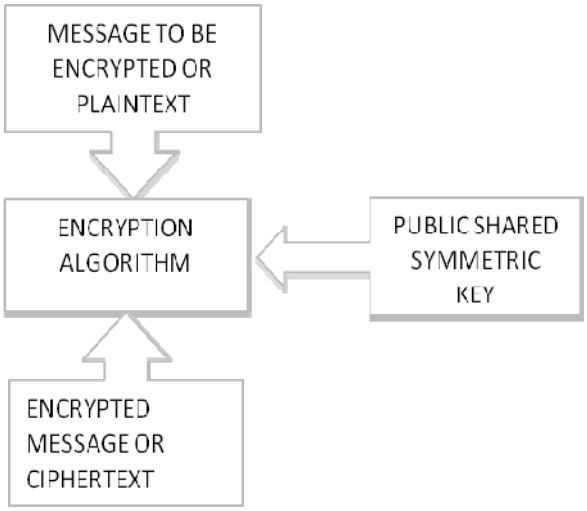

Fig 1.1.1 Encryption in Symmetric key Cryptography

It is used to enhance the security at various levels of network by using symmetric and assymetric mechanisms which are basically a part of modern cryptography which is different from tradiotional cryptography.

978-1-4673-7231-2/15/$31.00©2015 IEEE

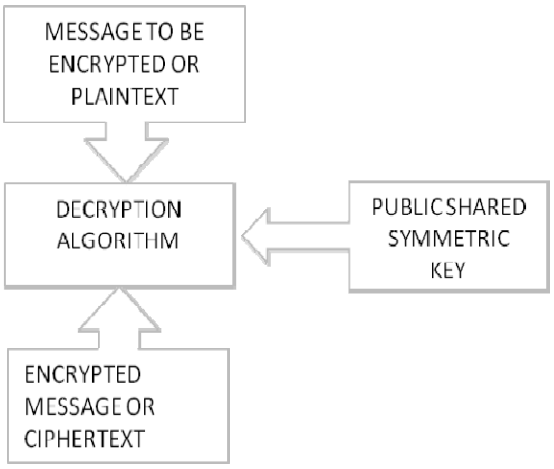

Fig 1.1.2 Decryption in Symmetric key Cryptography

In fig 1.1.1 and fig 1.1.2 defines the encryption and decryption using public hared symmetric key.The key is used at sender end for encryption and is used at reciever for decryption .However same key is used for both encryption and decryption and is not very secured mechanism.

Diagrammatic Representation of Private/Asyymetric Key Cryptography

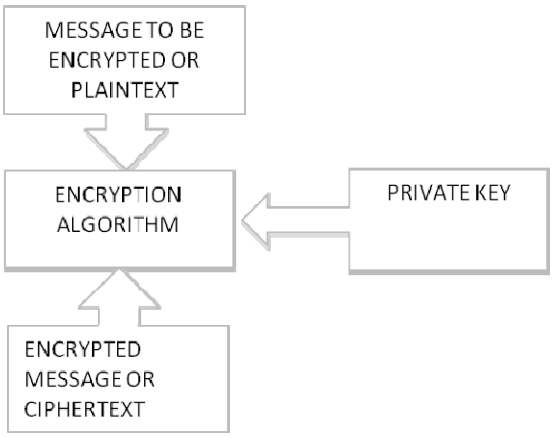

Fig 1.2.1 Encryption in Asymmetric key Cryptography

In fig 1.2.1 defines encryption using public key in asymmetric key Cryptography which any user or sender can do encryption using public key at the encryption end in aymmetric key cryptography[5].However, asymmetric algorithms are much slower than symmetric algorithms as it requires much more computation and therefore, in many applications, a combination of both is being used [6]. The asymmetric keys are used for authentication purposes and after this have been successfully completed; symmetric keys are produced and exchanged using the asymmetric encryption

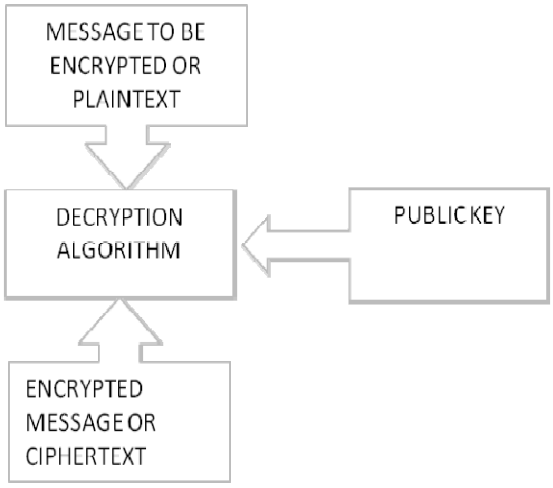

Fig 1.2.2 Decryption in Asymmetric key cryptography

Depending on the techniques[7] various authentication protocols are evolved challenge response protocol,public key protocol,symmetric key protocol(which uses Kerberos distribution)and diffie hellman key exchange protocol(which uses men in the middle attack).Depending on the security levels various keys are used over network to increase the security level[8].Hence, different research that has done toward text encryption and decryption in the block cipher.

II. PROPOSED MECHANISM

Existing framework have its drawbacks so proposed framework comprises of modules as under:

2.1 Public key-Public key technique.
2.2 Public key-Private key technique.
2.3 Private key-Public key technique.
2.4 Private key-Private key technique.

There exists symmetric and asymmetric key cryptography which uses public key and private key..Based on which various applications have been developed .However security issues have still not resolved.Hereinafter proposed framework uses the combination of public and private keys.The proposed framework has focussed on random combination of keys which is used for security enhancement[9].The main focus is to increase the complexity of system..The more the complexity is the higher is the security.

2.1 Public key-Public key technique: In this technique Encryption is done using public key and decryption is done using public key[10] .It is like the symmetric key cryptography technique but there exist the drawback that public key is easily accessible.It uses n:m relationship.

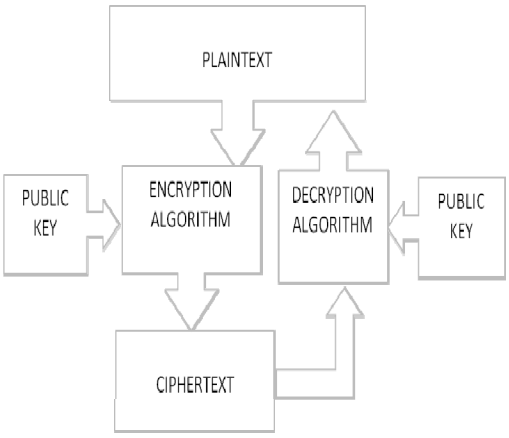

Fig 2.1 Public key-Public key Technique

Since the public key which is used both at encryption and decryption is public and can be easily accessible[6]The user at encryption is representated as n and at decryption is representated as m.Hence this model is not considered as very secure model.

2.2 Public key-Private key technique: In this technique Encryption is done using public key and decryption is done using Private key .It is like the asymmetric key cryptography technique but there exist the drawback that public key is easily accessible and private key is only known to reciever.[5]There can be many senders using public key ,but there exists only one reciever that uses private key.It uses n:1 relationship.In this public key is kept at encryption hich means there are n number of users and private key is kept at decryption which has one user which owns the private key[12].

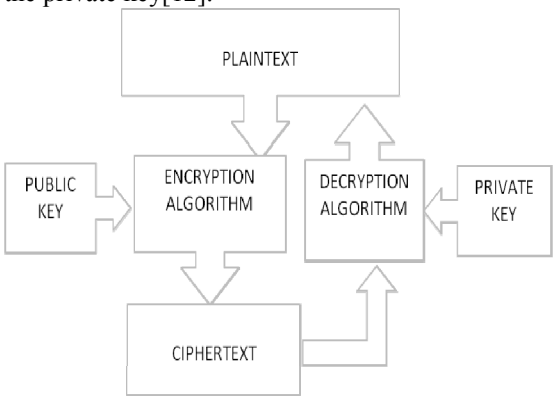

Fig 2.2Public key-Private key Technique

Henceforth two keys are used here public key at the sender end and private key at the receiver end .Public key at the sender end is accessible to all so it is common to all.It can be used by any user who has the access to the public key .Whereas private key is used at the receiver end which is specific to one user.The user who has the private key is the owner of data.Private key can be known to only one user so it is restricted to one user only.It means it is not accessed by multiple users.This is the basic concept of assymetric key cryptography.The complexity is more than previous model and has n:1 relationship.The complexity of this model makes it more powerful than previous model.

2.3 Private key-Public key-In this technique Encryption is done using private key and decryption is done using public key .It is unlike the asymmetric/symmetric key cryptography technique but there exist the drawback that public key is easily accessible and private key is only known to sender.[4]There can be many recievers using public key ,but there exists only one sender that uses private key.It uses a different combination of 1:n relationship.In Private key-public key technique private key is used at encryption and public key is used at decryption(n:1)The same combination is used in digital signature[9].However it has highest complexity and security.

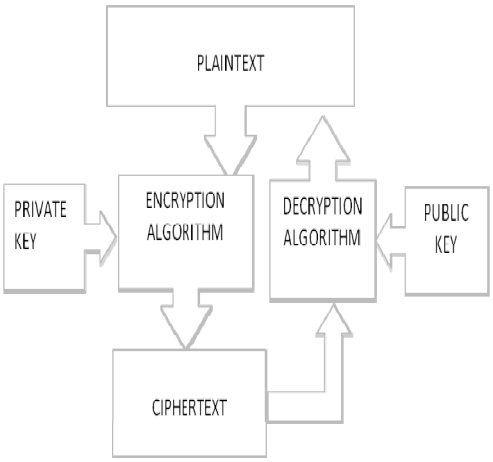

Fig 2.3 Private key-Public key Technique

2.4 Private key-Private key technique: In this technique Encryption is done using private key and decryption is done using private key[3] .This framework is the effective framework as it uses a private key at sender site and a private key at reciever ,both are different and secret .It is applied to one sender and one reciever[10] .It is used to transmit highly confidential data/information.It

uses a novel 1:1 relationship of keys.In this private-private key technique private key is used at encryption and a private key is used at decryption[7].The model has limited number of user which means one at encryption and decryption which means it is less prone to attacks like DOS,Spoofing etc.Henceforth,among all it is considered as the best modeland achieves higher security.

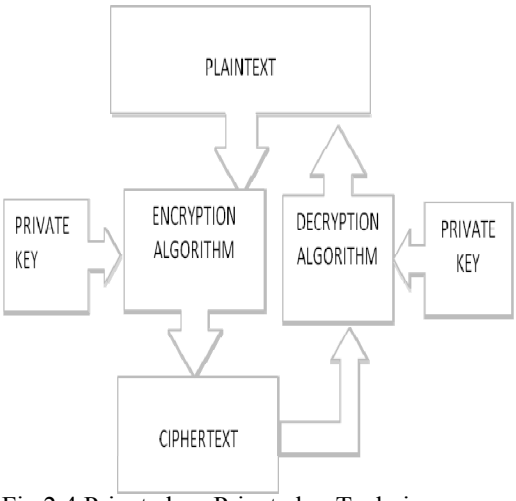

Fig 2.4 Private key-Private keyTechnique

III. RESULTS &COMPARISON

3.1 TABLEWISE

DEGREE	PUBLIC PUBLIC	PUBLIC PRIVAT	PRIVAT PUBLIC	PRIVAT PRIVAT
CONFIDENTIALITY	1	3	2	4
INTEGRITY	1	2	3	4
AUTHENTICATION	1	2	3	4
ACCESSIBLITY	1	3	2	4
NON-REPUTATION	1	2	3	4
ACCESS CONTROL	1	2	3	4

4=High Security
3=Medium Security
2=Moderate Security
1=Low Security

3.2 FIGUREWISE:

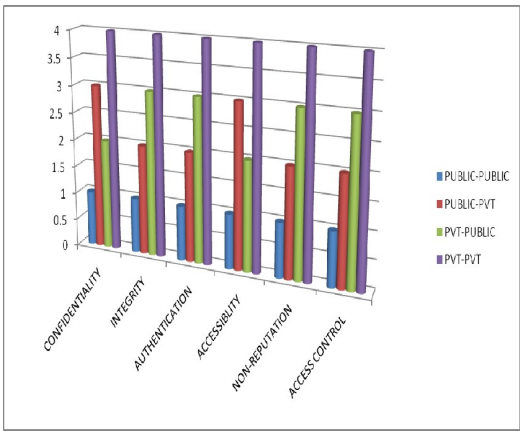

Fig 3.1 Comparison of Attributes of Information Security.

Private-Private key technique uses a private key at sender site and a private key at reciever ,both are different and secret .Data is more securely transmitted from sender to reciever.Based on the comparison of security mechansims all the parameters are achieved in private-private technique.Therefore it is considered as secure model.

IV. CONCLUSION AND FUTURE WORK

Private-Private key technique used to transmit highly confidential data/information.Data integrity is maintained and availability of right data to right users is also protected using this technique.Here confidentiality is also achieved.Since it is restricted with the keys so it is less prone to various types of attack like Dos,traffic analysis,spoofing etc.However this framework has also some limitations that are restriction to the number of sender and reciever that can be used for communication.Henceforth proposed cryptographic techniques are used for security enhancement. The information provided in this paper may be used for further researches and enhancements in the field of Cryptography.

ACKNOWLEDGMENT

This research was supported by Dr .Nitin Pandey in collaboration with Amity Institute of Information Technology,Noida

REFERENCES

[1] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, "Security and Privacy Enhancing Multi-Cloud Architectures", IEEE Transaction on Dependable and Secure Computing, Jan 2013.

[2] Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing", IEEE Communication Survey & Tutorials, Accepted for Publication, March 2012.

[3] Ayesha Malik, Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment", Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 3, March 2012.

[4] Mukesh Singhal and Santosh Chandrasekhar, "Collaboration in Multicloud Computing Environments: Framework and Security Issues", Published by the IEEE Computer Society, 2013.

[5] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom' "Cloud Computing Security: From Single to Multi-Clouds", International Conference on System Sciences, 2012.

[6] Kan Yang, Ren, Xiaohua Jia, Bo Zhang, and Ruitao Xie, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," IEEE 2013.

[7] P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, Tech. Rep., Sept 2011.

[8] Jing-Jang Hwang and Hung-Kai Chuang, " A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," National Science Council of Taiwan Government, IEEE ,2012International Journal on Advanced Computer Theory and Engineering (IJACTE) ISSN (Print): 2319-2526, Volume -3, Issue -4, 2014 10

[9] J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and =8L.L.L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds," Proc. IEEE Fourth Int'l Conf. Cloud Computing (CLOUD), 2011.

[10] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On Technical Security Issues in Cloud Computing," in Proceeding of IEEE Int'l Conf. Cloud Computing (CLOUD-II), 2009.3

[11] Kan Yang, Xiaohua Jia, " Attributed based Access Control for Multi-Authority Systems in Cloud Storage," in Proceeding of 2012 32nd IEEE International Conference on Distributed Computing Systems , IEEE ,2012

[12] M. A. AlZain, B. Soh and E. Pardede," MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing," in Proceeding of 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, IEEE,2011

[13] Selvakumar G. Jeeva Rathanam M. R. Sumalatha," PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique," IEEE,2012

[14] Akash Kumar Mandal, Mrs. Archana Tiwari, " Performance Evaluation of Cryptographic Algorithms: DES and AES," in Proceeding of 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, IEEE 2012

[15] J. D Assistant Professor, Ramkumar P Systems Engineer, Kadhirvelu D," Preserving Privacy through Data Control in a Cloud ComputingArchitecture using Discretion Algorithm," in Proceeding of Third International Conference on Emerging Trends in Engineering and Technology,IEEE,2010