International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 3 – MARCH 2016.

ENHANCED LEAKAGE RESILIENCY BASED SECURE DATA TRANSMISSION USING KEY ALLOCATION SCHEME SHUFFLING ALGORITHM

M.O.Ramkumar[1], G.Padhmavathi[2]

[1]*Assistant Professor, Department of Computer science and Engineering, IFET College of Engineering, Villupuram, India. Email Id: ramkumar.mo86@gmail.com*

[2]*B.E Student, Department of Computer Science and Engineering IFET college of engineering, Villupuram, India. Email Id: padhmaecofrnd@gmail.com*

***Abstract*- The leakage resilient cryptography is used to overcome SCA attacks, were external details such as power consumption, time taken to generate the key can be acquired by the attacker in order to get the parts of the secret key and then compute the leakage function to aggregate the secret key. This can be overcome using the concept of key updating. Thus key updating makes it impossible for the attacker to guess the exact key that is being generated. This paper is focused on perceiving before the malicious practices in the view of cryptographic schemes. We found the arrangement by proposing Key Allocation Scheme (KAS) with shufflingalgorithm. This plan lessened the impact of Certificates administration and produced abnormal state resistance without bargaining the peers. It is likewise managed to enhance the security with decreased communication cost using cryptographic schemes. As a foe can effectively send different types of assaults in the networks, at last we demonstrate that utilizing this strategy can upgrade the security of the system which builds the privacy and respectability.**

Keywords- Side Channel Assaults, Cryptographic schemes, Key Distribution Center, Encryption and Decryption

I. INTRODUCTION

Each center point fills in as a host and in addition a switch in the networks [1]. While getting data from the peers, the peer requires joint effort with each other to forward the data bundles, and this is known as Wireless Local Area Network [3]. This trademark gives a major issue from the parts of security. In fact, an application affects some stringent role on the security of the framework topology, routing and information activity [2]. For instance, the region and composed exertion of malignant peers in the framework may cut down the routing process that collapsesthe framework operations.

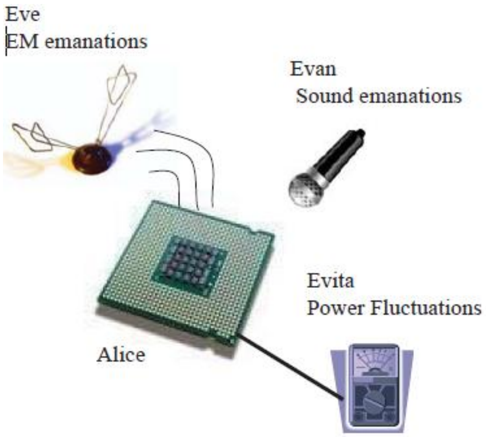


Fig.1. Side Channel Attacks [2]

The three pillars of SCA attacks were listed as:

- The leakage traces were affected by the sensitive variables.
- The hypothetical sensitive variables were estimated by Eve.
- The information can be combined from different traces.

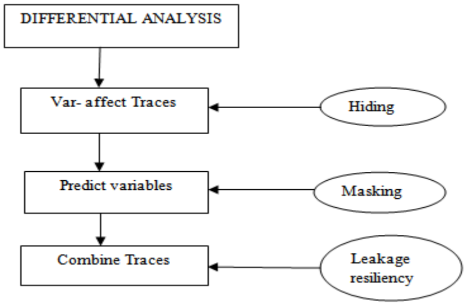


Fig.2. Pillars of attacks [1]

Hiding techniques depends on breaking the association between the intermediate variables and the recognizable spillage by minimizing the trace utilizing Signal to Noise proportion. This can be experts using balanced circuits and/or confusion generators. Disastrously, a cryptographic module utilizing hiding plansexpends a part of territory [4].

Masking depends on breaking Eve's ability to figure theoretical delicate variables, by a part of supportive information into n offers depending on subjective variable(s). The unpredictable variables are made on-the-fly and discarded immediately. Each offer is taken care of self-rulingly. The last yields (of each offer) are solidified to recuperate the primary yield. In this way, the cryptographic modules supported with masking require the twofold of the zone [5].

This paper is structured as: Section 1 depicts the Definitions of the SCA attacks and its importance in real world problems. Section 2 portrays the various studies conducted by the researchers in SCA systems. Section 3 proposes an innovative solution to the problem formulated from the previous studies. An innovative solution has been implemented and their outcomes were depicted in Section 4. Finally, it is concluded in Section 5.

II. LITERATURE SURVEY

Various investigation works have analyzed the issue of perceiving the malignant peers in MANETs. The greater part of these plans deal with the area of a solitary or large number malevolent center point, as far as time and cost for distinguishing the agreeable blackhole assaults. The discovery system recommended so far is delineated into two orders in particular, Proactive recognition plans and Reactive recognition plans. The proactive recognition plan [6] means to distinguish the noxious peers in a consecutive way. Responsive recognition plans are utilized to trigger the destination peers that recognize the huge drops of PDR (Packet Delivery Ratio) [7]. In [10], Liu et al, recommended 2ACK plan to foresee the bad conduct of routing in MANETs. In this arrangement, two-bounce affirmation parcels are sent to method for the routing to demonstrate that the data groups have been viably obtained. Zhou and Haas [8] at first prescribed edge cryptography to secure the MANETs, with edge signature [5], they proposed a Distributed Certification-Authority (D-CA) [7] to issue presentations to centers, D-CA are looked over center points in the framework. Lou et al. [9] proposed a plan of protocols for all inclusive and vigorous access control in MANETs. It additionally upgraded with better decision making process [5]. Saxena et al [10] added to a couple action of getting to control segmentsusing the Certificate based cryptography (CBC) and examined on existing edge marks.

An advance naturally raises the question whether certain block ciphers are better suitable for this purpose. In order to answer this question, we consider a leakage-resilient [14] re-keying function, and estimate its security at different construct levels. That is, we study possible attacks exploitdefinite features of the algorithmic description, hardware architecture and physical implementation of this construction. Technology (NIST) [11] promotes the U.S. economy and public welfare by providing technical management for the Nation’s dimension and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL’s tasks include the development of technological, physical, administrative, and management standards and rule for the cost-effective security and privacy of sensitive unspecified information in Federal computer systems.

A cryptographic primal is leakage-resilient, if it remains secure even if an adversary can learn aenclosed amount of random information about the calculation with every invocation. As a consequence, [12] the material implementation of a leakage-resilient primitive is secure against every side-channel as long as the quantity of information leaked per invocation is bounded.

III. SHUFFLING ALGORITHM- HEIGHTENED KEY ALLOCATION SCHEME

This proposed system analyzed on the efficiency of the secured data transfer of the dataspillage resiliency using shuffling algorithm based key allocation scheme. To address the security issues, it is very important to detect the malicious nodes. The algorithm is depicted in four approaches namely, User registration, Key authorities, Sender and User.

i) User Registration:

This is a versatile peer who needs to get into the information that put away at the storage peer (e.g., an officer). In the event that a peer has an arrangement of characteristics fulfilling the access policy of the encoded information characterized by the sender, and is not disavowed in any of the qualities, then he will have the capacity to decode the ciphertext and acquire the information.

ii) Key Authorities:

Key Generation is the process of creating keys using protection parameters to generate the secret key for the peers. The key is the combination of Message Sent Time (Ts) and the number of hops in the route (H_r).

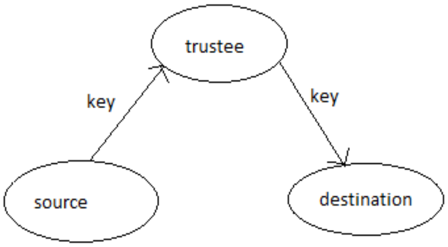


Fig.3. Key allocation scheme

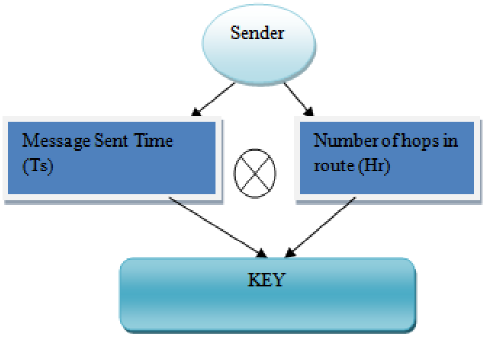


Fig.4. Formation of key

iii) Sender:

The translation of data into a ciphertext is known as encryption. Encryption is the most effective way to prevent data from leakage resiliency. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. It is also known as the Cipher text. The ciphertext is formed as:

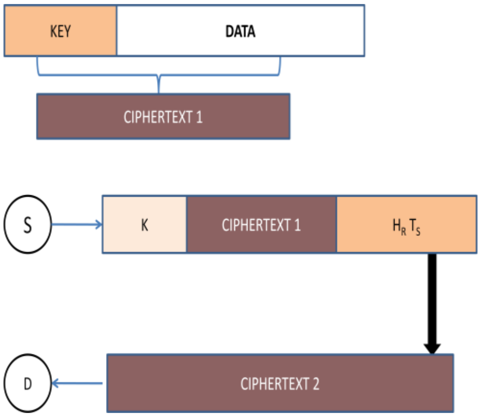


Fig.5. Encryption Process

iv) User:

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. The decryption is presented as:

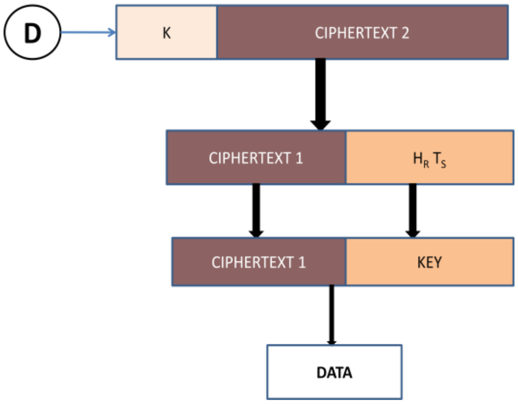


Fig.6. Decryption Process

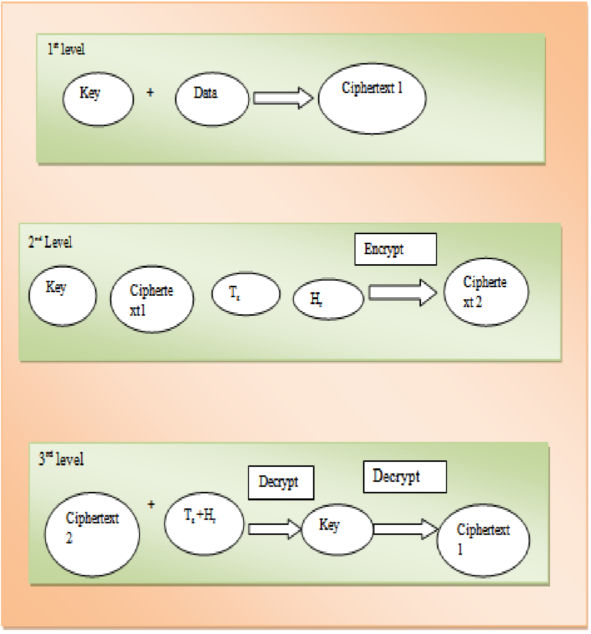
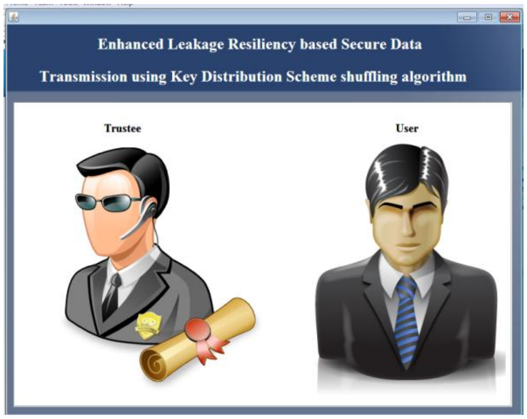


Fig.7. Proposed Architecture

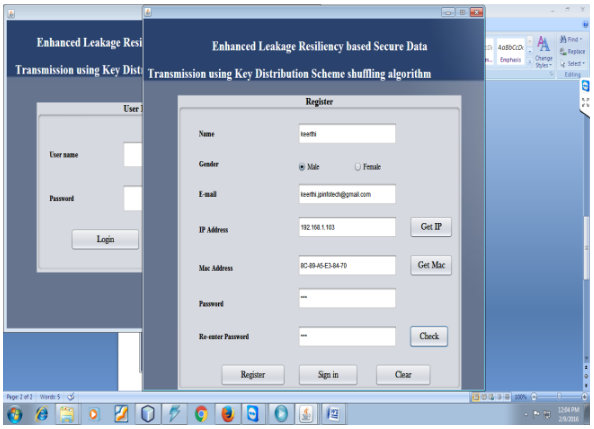
IV. EXPERIMENTAL DESIGNS AND RESULTS

A study was conducted using the key allocation scheme using shuffling algorithm. We employed a sample channel with data rate of 11 Mb/s. A random node is selected to inject the assaults in the network. Firstly, the proposed approach in design view is shown as follows:


Enhanced Leakage Resiliency based Secure Data

Transmission using Key Distribution Scheme shuffling algorithm

Fig. 8. Home page of the proposed system


Enhanced Leakage Resiliency based Secure Data

Transmission using Key Distribution Scheme shuffling algorithm

Register

Name: keerthi

Gender: ● Male ○ Female

E-mail: keerthi.jpinfotech@gmail.com

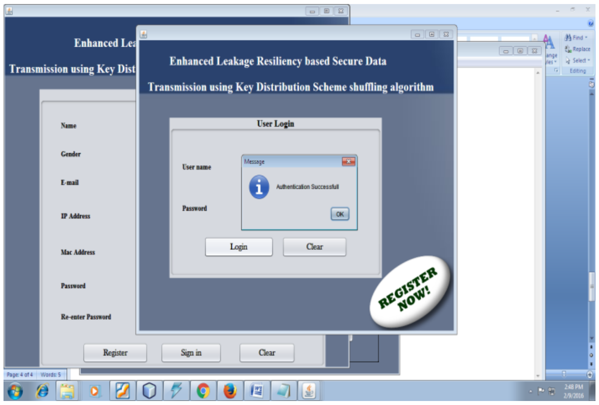
IP Address: 192.168.1.103

Mac Address: 8C-89-A5-E3-84-70

Password: ***

Re-enter Password: ***

Fig.9. User Registration


Enhanced Leakage Resiliency based Secure Data

Transmission using Key Distribution Scheme shuffling algorithm

User Login

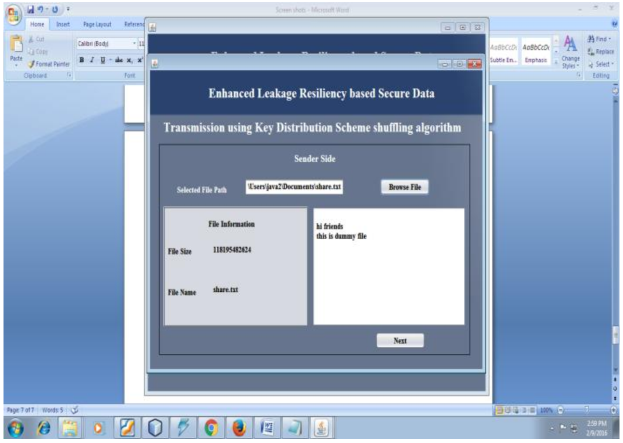
User name

Password

Message

Authentication Successfull

Fig.10. User Authentication process


Enhanced Leakage Resiliency based Secure Data

Transmission using Key Distribution Scheme shuffling algorithm

Sender Side

Selected File Path: \Users\java2\Documents\share.txt

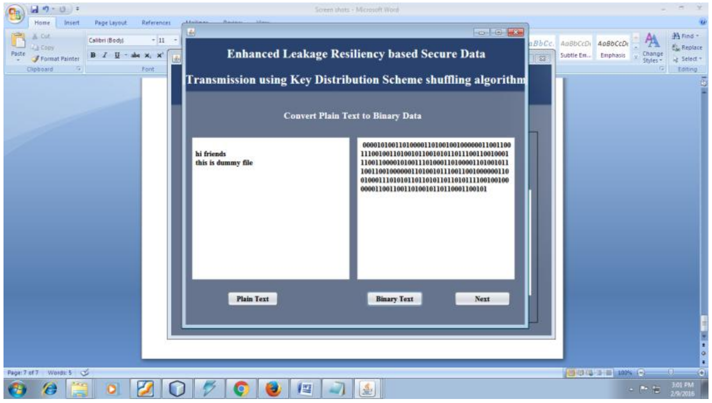
File Information

File Size: 118195482624

File Name: share.txt

hi friends
this is dummy file

Fig.11. Selecting the files from the sender side


Enhanced Leakage Resiliency based Secure Data

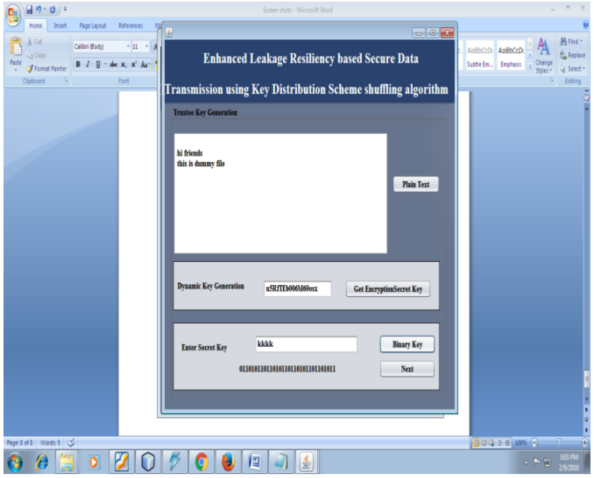
Transmission using Key Distribution Scheme shuffling algorithm

Convert Plain Text to Binary Data

hi friends
this is dummy file

```
000010100110100001101001001000000110011001
11100100110100101100101011011100110010001
11001100001010011101000110100001101001011
10011001000000110100101110011001000000110
0100011101010110110101011011010111100100100
0000110011001101001011011000110010 1
```

Fig.12. Conversion of plain text to binary data (encryption process)


Enhanced Leakage Resiliency based Secure Data

Transmission using Key Distribution Scheme shuffling algorithm

Trustee Key Generation

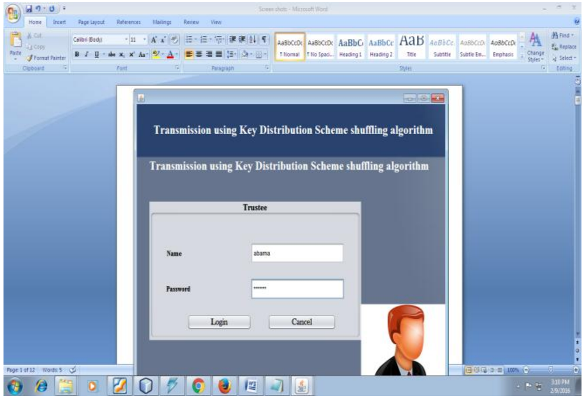
hi friends
this is dummy file

Dynamic Key Generation: u5RfTEb006M60osx

Enter Secret Key: kkkk

01101011011010110110101101101011

Fig.13. Generating the secret keys



Transmission using Key Distribution Scheme shuffling algorithm

Transmission using Key Distribution Scheme shuffling algorithm

Trustee

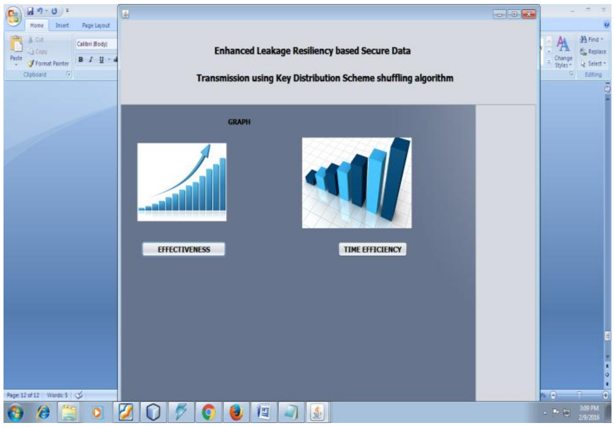
Name: abama

Password: ******

Fig.14. Activating the code in the trustee side

The performance metrics studied were:

i) ***Data Delivery Ratio:*** DDR is stated as the number of data received from the source to the destination to the total number of data originated in the source code.
ii) ***Throughput:*** In particular period of time, the number of messages delivered to the destination.
iii) ***Average End- End Delay:*** This is defined as the average time taken for a data to be transmitted from the source to the destination.



Enhanced Leakage Resiliency based Secure Data

Transmission using Key Distribution Scheme shuffling algorithm

Fig.15. Effectiveness and Time Efficiency

V. CONCLUSION

Key administration assumes an essential part in cryptography as the premise for securing cryptographic systems that provides privacy, entity validation, information origin validation, information integrity, and computerized signatures. The objective of a decent cryptographic outline is to decrease more mind boggling issues to the correct administration and safe-guarding of a smaller number of cryptographic keys, at last secured through trust in equipment or programming by physical detachment or procedural controls. Dependence on physical and procedural security (e.g., secured rooms with detached hardware), tamper-resistant equipment, and trust in countless people is minimized by concentrating trust in smaller number of effortlessly checked, controlled, and dependable components.

REFERENCES

[1] MostafaTaha, Member, IEEE, and Patrick Schaumont, Senior Member, IEEE, "Key Updating for Leakage Resiliency With Application to AES Modes of Operation", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March , 2015

[2] P.-C. Tsou, J.-M.Chang, H.-C.Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chennai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[3] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013).

[4] C. Chang, Y.Wang, and H. Chao, "An efficientMesh-based core multicast routing protocol onMANETs," J. Internet Technol., vol. 8, no. 2, pp. 229–239, Apr. 2007.

[5] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996.

[6] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in Proc. IEEE Aerosp. Conf., 2002, vol. 6, pp. 2727–2740.

[7] A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.

[9] K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.

[10] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[11] M. Dworkin, "NIST special publication 800-38A, recommendation for block cipher modes of operation: Methods and techniques."

[12] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Efficient and highperformance parallel hardware architectures for the AES-GCM," IEEE Trans. Comput., vol. 61, no. 8, pp. 1165–1178, Aug. 2012.

[13] Y. Dodis and K. Pietrzak, "Leakage-resilient pseudorandom functions and side-channel attacks on Feistel networks," in Proc. 30th CRYPTO, pp. 21–40, 2010.

[14] S. Belaïd et al., "Towards fresh re-keying with leakage-resilient PRFs: Cipher design principles and analysis," J. Cryptograph. Eng., vol. 4, no. 3, pp. 157–171, Sep. 2014.

[15] P.Manju Bala , M.O.Ramkumar Analyzing Security of Single Sign on System through Advanced Encryption Standard IJCCTS .,vol. 2, issue 6 Aug-2014.