Enhanced Secure Data information over Network using DES

K. Arul[1] M. Sakthilvel[2]
[1]PG Scholar [2]Assistant Professor
[2]Department of MCA
[1,2]Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College

Abstract— Security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Security measures mostly which involve data encryption and private passwords. Many issues arises due to privacy of information, security of that information will be misused. Consists of the provisions made in an underlying computer network security infrastructure which adopted by the network administrator to protect the network and network accessible resources from unauthorized access and the effectiveness (or lack) of the measures combined together. The main goal is to perform security technologies while protecting the data or message of each of the owners from the other owners without revealing any leakage of information. In the first case, the goal is to protect the data information or message from unsecure network. Here we introduce some techniques for authorized person to access their information without any theft using security methodology of Data Encryption Standard and their concerns.

Keywords: Security Protocols, Data Encryption Standard, Cryptographic protection

I. INTRODUCTION

The Data information has also been hard to keep over the distributed system. In previous work the data are maintained through some private key mechanism. In any case, the internet is definitely an open network .once data is transmitted beyond the organizational network, which may be handled by any n number of different intermediate computers (called routers) which make sure the data is delivered to its intended destination. Data is also likely to travel across internet backbone networks, which move vast quantities of data over large distances.

A. Internet Fundamentals

At the most fundamental level, the Internet is a series of standards for three basic tasks are: Sharing a file with one or more parties, sharing email with one or more parties, allowing the user of one computer system to log onto another computer system. The greatest threat to security in any system almost invariably comes from within. There are still some serious risk factors of while transmit data across the internet. The internet is open-meaning transmissions can be overhead, interception by third party, forgery and modification.

II. EARLIER APPROACH

Internetworking protocols and cryptography don't make easy reading, but they do build a base for understanding the issues. Interception of network traffic is only a problem of sending sensitive information. Forgery can be a much more serious risk. The email protocols make s it a relatively simple matter for someone to send a message that appears to be coming from someone else. Another insidious threat is that someone will intercept transmissions, modify them and send them on to their destinations. However the risks over the open link inherent in communication. Information is vulnerable at many points, including the originating system(which may have been tampered with at same point to subvert it) the local or organizational network (local traffic is almost trivially easy to listen to and required little more than a connection to the same network) and some intermediate system or network out on the internet .The service provider not implemented sufficient security to prevent the attack, which apparently had not taken advantage of any inherent internet weakness, but exploited security weakness in the actual system.

III. PROPOSED METHODOLOGY

The proposed which improves the problem in existing .In terms the way of data information moves around the internet itself is unreliable and unsecure-but can still allow reliable and secure message to be sent and received. These describe how the data information is being maintained using security technologies. An efficient protocol has been used to protect the data through security techniques. The protocol depends on Data encryption standards, cryptographic primitives these extract and maintain the information through secure manner in open environment. The systems to keep records and collect data, the informed user are examining what information is solicited, what is shared and what is kept private. They are useful in the design of internetworks because they separate and distribute important functions in efficient way .The specific type of network cable that is connected to system is a vital part of internet traffic but only as it concerns moving that traffic from the internet service provider to actual system. It means that no intermediate routers need to worry about the reliability or security of the data they transfer from network to network. This would mean additional computations for verifications they just make sure it arrives at its destination. Once the data reaches its destination, the target computer can then make sure the data it receives is reliable and secure.

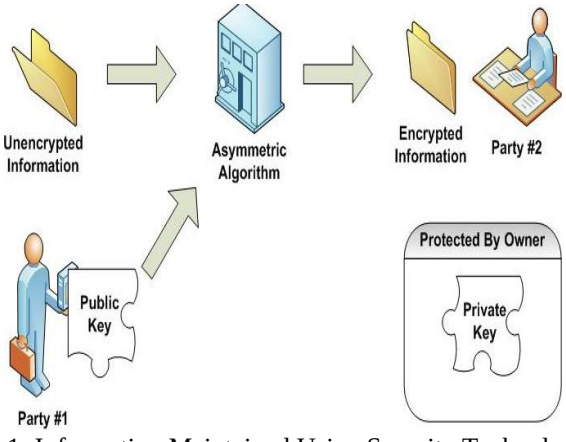

Fig. 1: Information Maintained Using Security Technologies

IV. SYSTEM ARCHITECTURE

A widely distributed secret key solution is the Data Encryption Standard. It specifies Cryptographic algorithm which provides a complete description of a mathematical algorithm for encrypting and decrypting binary coded information. Encryption data converts it to an unintelligible form called cipher. Decrypting data that converts back to its original form called plain text. The algorithm describes in this standard specifies both encryption and decryption cipher operations which are based on binary number called a key.

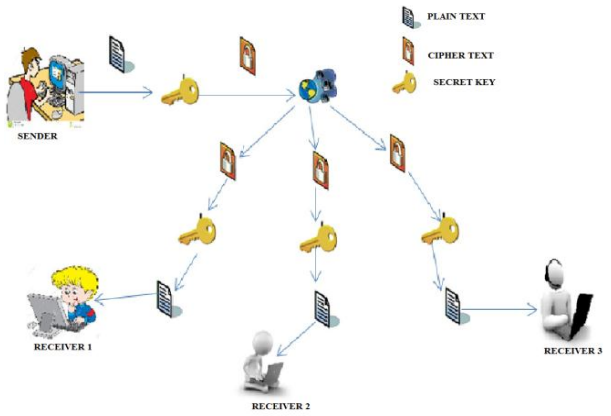

Fig. 2: Architecture Diagram

V. DATA ENCRYPTION STANDARDS (DES)

A key consists of 64 binary digits (0's and 1's) of which 56 bits are randomly generated and used directly by algorithm. The other 8bit, which are not used by the algorithm, are used for error detection. The 8bit error detecting bits are set to make the parity of each 8bit byte of the key odd, which is there is an odd number of "1" in each 8bit byte. Authorized users of encrypted data must have the key that was used to encipher the data in order to decrypt it. The secret key chosen for use in a particular application makes the result of encrypting data using the algorithm unique. The cryptographic security of the data depends on the security provider for the key used to encipher and decipher the data. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data. Data that is considered sensitive by the responsible authority, data that has a high value should be cryptographically protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while storage.

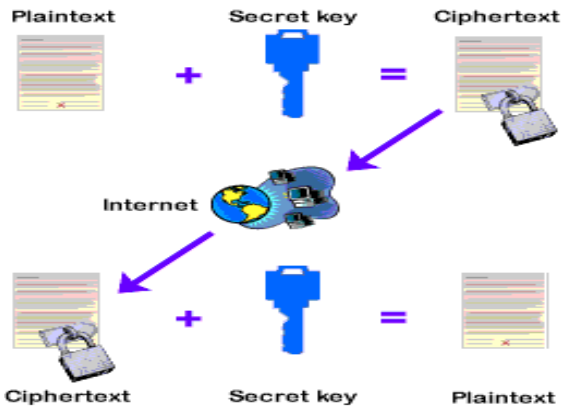

Fig. 3: Sharing Secret Key over Network

A. Encryption and Decryption Algorithm

Data encryption is utilized in various application and environments. The specific methodology of encryption and the implementation of the DES will be based on many factors particular to the computer system and its associated related components. Basically, cryptography is used to protect data while it is being communicated between two points or while it is stored in a medium vulnerable to physical theft. The communication security provides protection to data by enciphering it when it is transmitting point and deciphering it when it is receiving point. File security which provides protection to data by enciphering it when it is recorded on a storage medium and deciphering it when it is read back from the storage medium. In the first setting, the key must be available at the transmitter and receiver simultaneously during communication .In the second setting, the key must be maintained.

B. Cryptographic Security Protection

DES specifies Cryptographic modules which implement FIPS (Federal Information Processing Standards).The specific implementation may be depend on several factors such as the application, the environment, the technology used some techniques. Implementation which may include electronic devices, microprocessors using Read Only Memory(ROM), Programmable Read Only Memory(PROM),Electronically Erasable Read Only Memory(EEROM) and Mainframe computers using Random Access Memory(RAM).

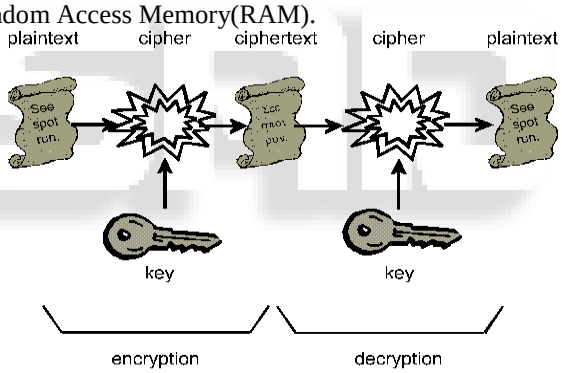

Fig. 4: Cryptographic Protection Using Alternative Methods

VI. CONCLUSION

Data encryption in terms of security which translates of data into a form that is unintelligible without deciphering mechanism. A password is a secret word or a phase that gives a user to access their confidentiality of data over network without any Interception by third party and forgery. These standards providing cryptographic protection using alternative methods and conclusively proven from secure attack.

REFERENCE

[1] Feis75 Feistel, H. Notz, W. and Smith, J., "Some Cryptographic Techniques for Machine-to-Machine Data Communications," Proceedings of theIEEE, November (1975).
[2] Pfleeger, C., "Security in Computing, Upper Saddle River," NJ: Prentice Hall, (2002).
[3] Li Juan, Chen Bin, and Li Kun, "Study on the Improvement of Encryption Algorithm of

Bluetooth," International Conference on Networking and Digital Society. pp. 89-92, (2009).
[4] Coppersmith, D., "The Data Encryption Standard (DES) and Its Strength Against Attacks," IBM Journal of Research and Development, May (1994).
[5] Electronic Frontier Foundation. "Cracking DES:Secrets of Encryption Research, Wiretap Politics, and Chip Design," Sebastopol, CA: O'Reilly, (1998).
[6] Menezes, A., van Oorschot, P., and Vanstone, S, "Handbook of Applied Cryptography," Boca Raton, FL: CRC Press, (1997).
[7] Schneier, B., "Applied Cryptography," New York: Wiley, 1996. Simovits, M., "The DES: An Extensive Documentation and Evaluation," Laguna Hills, CA: Aegean Park Press, (1995).
[8] Stinson, D., "Cryptography: Theory and Practice," Boca Raton, FL: CRC Press, (2002).
[9] Shamir;"How to share a secret," Communications of the ACM, vol.22 (11), pp.612–613, 1979.
[10] Jaiwei Han and Micheline Kamber, "Data Mining-Concept and Techniques", Morgan Kaufman Publishers, 2nd Edition , 2006.
[11] Moez Waddey , Pascal Poncelet, Sadok Ben Yahia, "Novel Approach For Privacy Mining Of Generic Basic Association Rules," In PAVLAD'09, November 6, 2009, Hong Kong, China, 2009 ACM.
[12] Xuan Canh Nguyen, Hoai Bac Le, Tung Anh Cao, "An Enhanced Scheme For Privacy-Preserving Association Rules Mining On Horizontally Distributed Databases," In IEEE 2012.
[13] N. V. Muthu Lakshmi1 & K. Sandhya Rani, "Privacy Preserving Association Rule Mining in Vertically Partitioned Databases," In International Journal of Computer Applications (0975 – 8887) Volume 39– No.13, February 2012.
[14] M. Kantarcioglu and C. Clifton. Privacy-preserving distributed mining of association rules on horizontally partitioned data. IEEE Transactions on Knowledge and Data Engineering, 16:1026–1037, 2004.

