ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Transmission via Air Gap Networking

B.Bhavana
B.Tech Scholor
Dept. of Information Technology,
Vignana Bharathi Institute of Technology,
Aushapur, Hyderabad-501301.

P.Harsha Reddy
B.Tech Scholor
Dept. of Information Technology,
Vignana Bharathi Institute of Technology,
Aushapur, Hyderabad-501301.

B.Kruthika Reddy
B.Tech Scholor
Dept. of Information Technology,
Vignana Bharathi Institute of Technology,
Aushapur, Hyderabad-501301.

Mr.V.Sridhar Reddy
Associate Professor,
Dept. of Information Technology,
Vignana Bharathi Institute of Technology,
Aushapur, Hyderabad-501301.

ABSTRACT

Secure transmission refers to the transfer of data such as confidential or proprietary information over a secure channel. Many secure transmission methods require a type of encryption and decryption. The most common email encryption is called PKI. In order to open the encrypted file an exchange of keys is done.

Keywords: ***Decryption, Encryption, Internet, cryptography, AES, MD5.***

INTRODUCTION

A collaborative usage of both software and hardware has led to the development of this particular technology. When the need for accessing the internet and transferring the data, in an asynchronous manner ,from one system to another system, arise , security comes into the scenario. The PCs usually having internet connection do not have the RCnet/intranet connection, and vice versa.

Due to this, an interface is created that helps in easy access of data from an open source and transferring of that data from one device to another. In this the hardware follows the RS-232 protocol, and the software is developed in DotNet. An encryption method is used, where the data downloaded is first encrypted using Hash Function, encryption technology. It is a key that is generated to encrypt or decrypt that particular file using this particular process of cryptography.

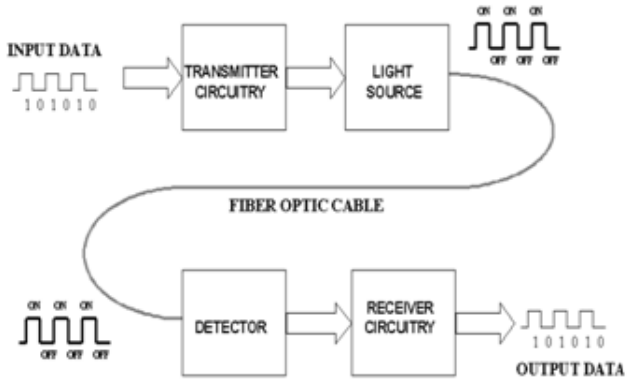
A brief of the data transfer interfaces are as follows

1) USB to Serial Converter
2) Serial to Transistor-Transistor Logic Converter
3) Transistor-Transistor Logic to Optical Converter
4) Optical Transmitter
5) Optical Receiver
6) Optical to Transistor-Transistor Logic Converter
7) Transistor-Transistor Logic to Serial Converter
8) Serial to USB Converter

When a file is downloaded from the internet, it is encrypted using cryptography. In cryptography, MD5 is a cryptographic Hash Function, designed by the NSA(National Security Agency). This function develops a varied range of 128/192/256 bits message digest algorithm, which is also called the key. In addition the AES cipher is used,this means the same key is used for both encryption and decryption. The data files are transferred to serial converter, through a USB port. The serial converter transports this data file to the TTL converter using several ICs, from where it is conveyed to an optical converter. This optical converter has a transmitter and a receiver. The transmitting end can only transmit, and n. There is a special usage of a CCD(charge couple device). This is a device that is by far the best mechanism to convert optical images to electrical signals. This safeguards the file as it cannot be moved from one end of the transmission path to the other due to optical transference which is a one way mode. The optical transmitter takes the data in the form of an electrical signal and converts it to an optical signal, which is

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

then transmitted in the form of an EM wave and is detected by the receiver. The receiver takes the optical signal and generates electrical pulse



The optical converter then follows the same process and transmits the file to the TTL converter, which is then transferred to a serial converter, from where the file is further transferred to the desired device using a USB port.

LITERATURE REVIEW

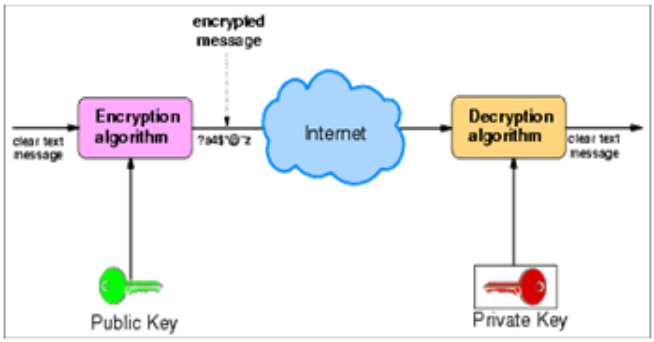
Security plays an important role in our life as well as in the area of networking for transmission of data from one device to other device, because it is only responsible for securing all information which are passed through the computers network. Cryptography is a concept to protect network and data transmission over network. It is an emerging technology which is very important for network security, data securing is the main aspect of secured data transmission over unreliable network. Data securing is a challenging issue of data communication today that touches many areas including secured communication channel, strong data encryption technique and trusted third party to maintain the database. The convention method of encryption can only provide the security; the data could be accessed by the unauthorized user for malicious purpose. Therefore it is necessary to apply effective encryption/decryption method to enhance data security among the security mechanism like Firewall, VPN (Virtual Private Network), authentication and cryptography the most securing strategy is cryptography. Cryptography cover the area of authentication and encryption, ciphers is very important in cryptography, in symmetric key a key called secret key is used for both encryption and decryption but in the case of asymmetric ciphers which is consist of two keys namely private key and public key in the process of encryption we deals with lots of algorithms like DES, AES, RSA, MD5, etc.

DES is a secret key algorithm, RSA is a public key algorithm, MD5 is ideal for authentication purpose so the main goal of network security is to provide a platform so that the data send by the sender is to be produce in the same order to the receiver without affecting the original form of data. It is very essential in network security to maintain the integrity of data and for this encryption play an important role to achieve this task as data is always a big asset for any organisation and keep these data secure for long time is a big challenge for organization. In that case encryption is a very good candidate to provide the security over the transmission of data in a network.

Security is essential factor during communication among the people and in e-commerce for the internet user applications such as private communication, password protection and secured e-commerce [1]. The need of secure communication i.e., with Cryptography techniques provides high security like internet banking, ATM's and Satellite transmission etc.

Cryptography concept provides the security to store secret and sensitive data, to transmit to receiver by sender and vice versa.Cryptography is the concept of mixing the complex mathematics and logical functions for the process of encryption and decryption of the message. The degree of security is dependent on the key and strength of the algorithm which are used to encrypt and decrypt the plaintext (message).the cryptography is classified into mainly two types and they are based on the key. Two types of cryptography namely secret (symmetric) and public (asymmetric) key cryptography and the following Fig1 shows the classification Fig1: Classification of Cryptography.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



A. Private key Cryptography: in this process we use same key to encrypt and decrypt data of the message i.e., the symmetric key hence it is also termed as symmetric key cryptography.

B. Public key Cryptography: in this process we use different keys for encrypt and decrypt data of the message i.e., the asymmetric key hence it is also termed as asymmetric key cryptography.

III. MOTIVATION

It is a guaranteed one way network connection, which protects secrets and safeguard availability and integrity of critical assets.

It can be conveniently used by the government and its defense organizations, as it provides zero compromise on security. Security and confidentiality of informations is very vital, because of which more than often isolated networks or intra-networks are developed and used. But with this technology no such measures are required as it provides immediate protection, confidentiality and availability.

AIR GAP NETWORK

Air gapping is a security measure that involves isolating a computer or network and preventing it from establishing an external connection.

An air gapped computer is physically segregated and incapable of connecting wirelessly or physically with other computers or network devices. To to prevent unauthorized data extrusion through eletromagnetic or electronic exploits, there is often a specified amount of space between the air gapped system and outside walls and between its wires and the wires for other technical equipment.

The U.S. National Security Agency TEMPEST project provides recommendations for air-gapping security measures. For a system with extremely sensitive data, a Faraday cage can be used to prevent electromagnetic radiation (EMR) escaping from the air-gapped equipment. Although these measures seem extreme, van Eck phreaking can be used to intercept data such as key strokes or screen images from demodulated EMR waves, using special equipment from some distance away. Other proof-of-concept (POC) attacks for air gapped systems have shown that electromagnetic emanations from sound cards on isolated computers can be exploited and continuous wave irradiation can be used to reflect and gather information from isolated screens, keyboards and other computer components. Acoustical-infections have been demonstrated that will transmit data from an infected air gapped computer over ultrasonic frequencies to computers outside the air gap. Air-gapping is used in the military, government and financial systems like stock exchanges. The measures are also used by reporters, activists and human rights organizations working with sensitive information.

Air gapping can also be used to maintain a stable software environment for sensitive application development. Some very simple computerised control mechanisms are also air gapped in this case because they are self-contained and simply do not require outside control. Examples include computerised thermostats that regulate heating and cooling, sprinkler systems, nuclear equipment and engine control units.

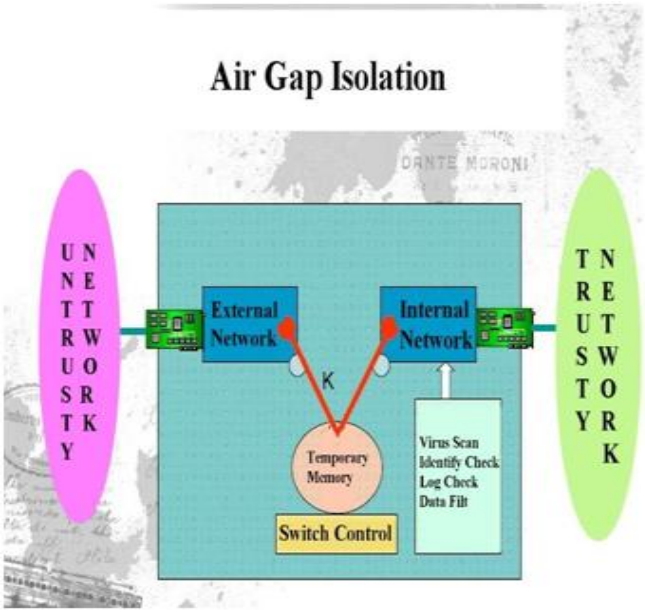
The software-defined perimeter (SDP) framework is sometimes referred to as a method of virtual air gapping. SDP requires authentication of all external endpoints attempting to access internal infrastructure and ensures that only authenticated systems can see internal IP addresses.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

EXAMPLES

1.Military/governmental computer networks/systems;
2.Financial computer systems, such as stock exchanges;
3.Industrial control systems, such as SCADA in Oil & Gas fields;

Visual representation of a typical air gap network:

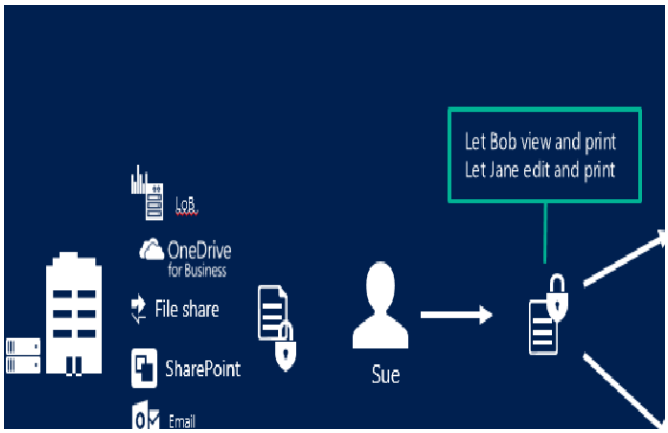


IV. IMPLEMENTATION

1.Essentially, we implement techniques such as hashing and message digest to provide security.
2.We make use of symmetric key cryptography in order to facilitate encryption.
3.We are also utilizing database validation in order to store records of authentic users.
It is a guaranteed one way network connection, which protects secrets and safeguard availability and integrity of critical assets.

It can be conveniently used by the government and its defense organizations, as it provides zero compromise on security. Security and confidentiality of informations is very vital, because of which more than often isolated networks or intra-networks are developed and used. But with this technology no such measures are required as it provides immediate protection, confidentiality and availability.

This sort of data diode, is extremely reliable , with zero failure as it undoubtedly provides unidirectional data transfer. Also this one way connection provides 100% security. Any addition and automation can be done to the data without having to compromise it's security.



Control systems are created in industrial level for developmental purposes, however such systems are often breached because of malicious intent. Because of this reason the systems are either delayed or disrupted. But with this technology of data diode, the data can be shared without danger of exposing critical contents.

V. METHODOLOGY

CURRENT WORK SCENARIO:

1) SOFTWARE
2) HARDWARE

SOFTWARE:

Use of Hash function:

A hash function is an efficient function mapping binary strings of arbitrary length to binary strings of fixed length, called the hash value or digest. A hash function must be one way. Given only a digest it must be computationally infeasible to map the same digest. A collision is a situation where two different messages F and F' such that the digest thus creates a unique fingerprint of the data.

This method uses the method of generating a special function H, not based on a block cipher. There are multiple types of hash functions. This particular

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

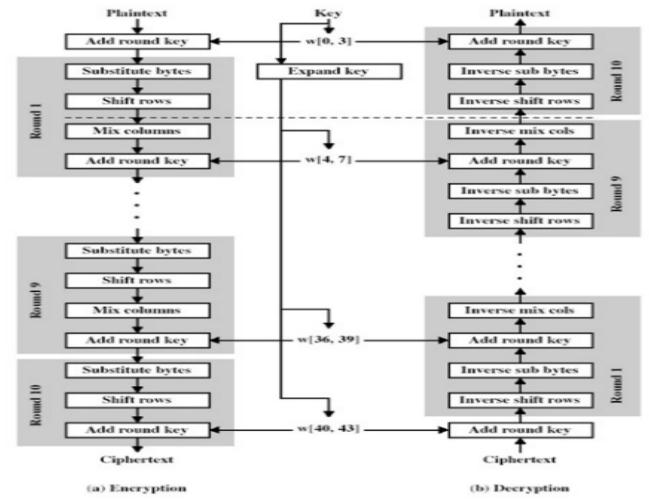
method uses the MD5 family (message digest algorithm). In hash function the output is always smaller than the input. There are multiple usage of the hash function.

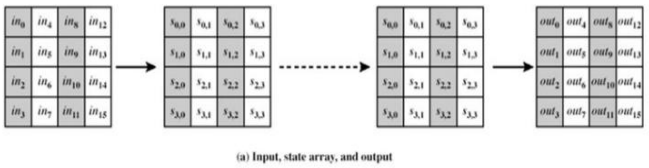
APPLICATION

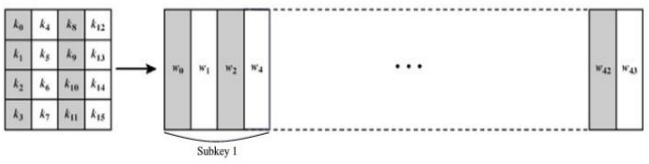
It is used to encrypt the digest with a private key. Digest of password is compared

Use of AES cipher:

The AES is a symmetric block cipher. It means that it uses the same key for both encryption and decryption. The block and the key can be of any chosen independently of any chosen sizes. Choice of three keys can be used - 128,192, 256 bits. Depending on which version is used the names are given as follows AES-128, AES-192, AES-256. The input is a single 128 bit block and is often known as the in matrix. This block is copied into a state array, which is modified at each stage of the algorithm, and then copied to the out matrix.



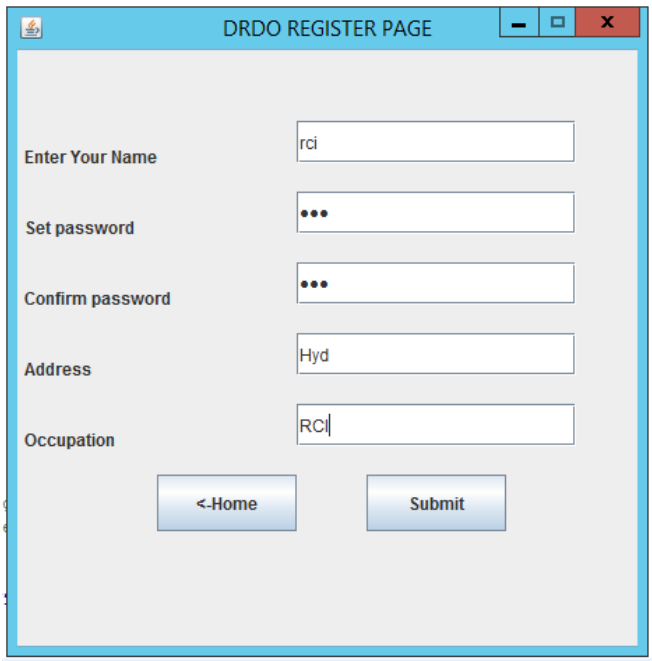

(a) Input, state array, and output

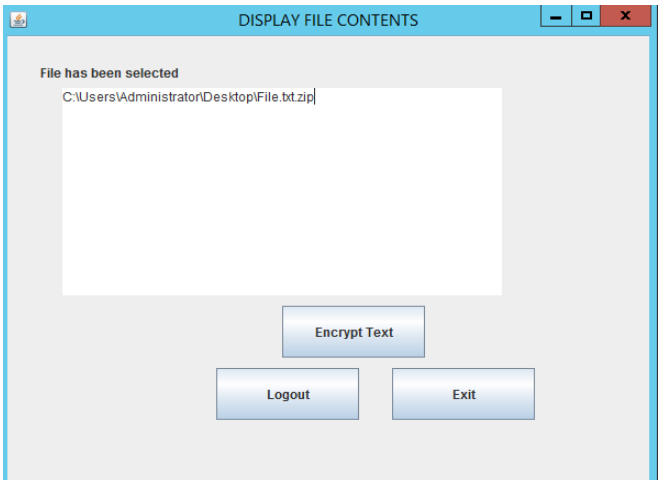


(b) Key and expanded key

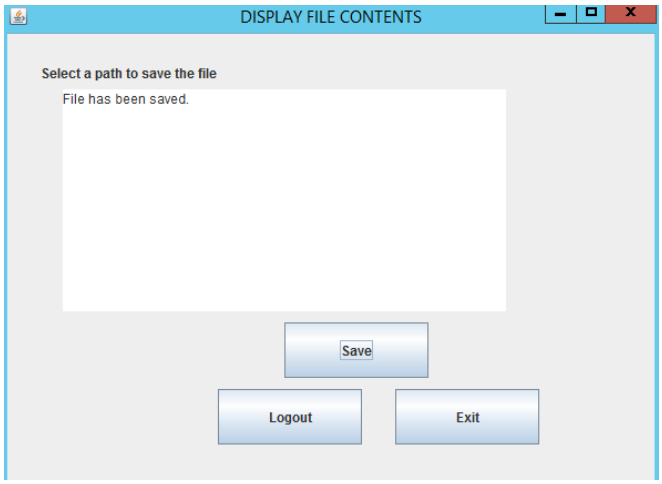
VI. RESULT

Below figures are the results





ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



VI. CONCLUSION

In conclusion, this project is highly usefulhis project is highly useful in order to transmit data through simplex or half duplex communication.

We avoid connection to any networks and hence maintain the integrity of the air gap network.

Any upgradation is done via serial-usb data transfer and thus we are completely isolating our network and protecting it from malicious data.

The confidentiality, integrity and authenticity of our data is maintained and data leakage or loss is avoided.

VII. REFERENCES

1.Z. Hrytskiv, S. Voloshynovskiy& Y. Rytsar "Cryptography of Video InformationIn Modem communica-tion", Electronics And Energefics, vol.11, pp. 115-125, 1998

2.Wheeler D., and R. Needham. TEA, a Tiny Encryption Algorithm, Proceedings of the Second International Workshop on Fast Software Encryption, Springer-Verlag, 1995, pp. 97-110.

3.National Institute of Standards, Data Encryption Standard, Federal Information Processing Standards Publication 46. January 1977

4.Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

5.Chandramouli, R., Kharrazi, M. &Memon, N., "Image Steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

6.Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston. London, 2000.

7. Marvel, L.M., Boncelet Jr., C.G. &Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999