SECURED DATA PACKET TRANSMISSION BY USING THE RGB COLOR CODING TECHNIQUE FOR COMPUTER NETWORK

[1]Vaibhav Kant Singh, [2]Devendra Kumar Singh
[1]Department of Computer Science & Engineering, Institute of Technology
Guru Ghasidas Vishwavidyalaya, Central University, Bilaspur,C.G,India
Email: [1]vibhu200427@gmail.com , [2]devendra.singh170@gmail.com

Abstract—In the age of Internet surveillance, private and secure messaging is a necessity. Hijacking or man-in-the-middle attack is a class of attacks where the hacker begins by listening in on the electronic conversation between two communicating hosts. No matter how much secure a system is made, there would be attackers, who would constantly try to find their way. We call them intruders, because they try to intrude into the privacy of a network. Whether the network itself is private (e.g. a Local Area Network) or public (the Internet) does not matter. What matter is the intent of the attacker, of trying to intruders? It is generally said that the two most widely known threats to security are intruders and viruses. We shall concentrate on intruders here. Intruders are said to be of three types. As explained below:

- **Masquerader: A user who does not have the authority to use a computer, but penetrates into a system to access a legitimate user's account is called as a masquerader. It is generally an external user.**
- **Misfeasor: There are two possible cases for an internal user to be called as a misfeasor:**

A legitimate user, who does not have access to some applications, data or resources, accesses them. A legitimate user, who has access to some applications, data or resources misuse these privileges.

- **Clandestine user: An internal or external user who tries to work using the privileges of a supervisor user to avoid auditing information being captured and recorded is called as a clandestine user.**

For the last decade, e-mail worms have been the number one threats on the computer system, especially windows system. Most worms arrive as a file attachment or as an embedded script that the end users execute. So we want significantly decrease network exposure risk by packet secured by intruders using RGB intensity values. So we want to build an application that is able to send and received encrypted text/images or messages data. According to our application the user has skill to choose the counterfeit text he wants and the program or application must be able to tell the text/image or messages whether or not these counterfeit text/images or messages will ensembles the real text.

Index Terms—Security, Intruder, Third Party.

I. INTRODUCTION

Security has always been a very important issue for all type of computer applications, especially Web based applications. Web based applications are easy to get to the almost entire world, and are chance for assail. Most of the web based applications gives the file downloading feature, the real time challenge is not in providing such a feature, but in securing such operations. We give an application which demands for secure file upload and downloading during the internet.

There are two types of attack for: active and passive version in a active version of the man-in–the-middle utilize to assume control of communication path to sabotage the normal functionality of the network the attack may redirect the information to the hacker, modify the information to suite the attackers need or prevent transmission of data one of the strongest and common form of such attack is the replay attack. That type of attack may obtain attack the information being passed through the network via network sniffers and can relay the information at a later time to obtain excess of a certain system. For example, the attacker can obtain an encrypted message and may used to satisfy a protocol at a later time simply by relaying the information here the important thing such attacks do not even need the decoding the information. Passive attacks are the nature of eavesdropping on, or monitoring of transmission. The goal of the opponent is to obtain information that is being transmitted [Berouz Forouzan]. We are sending and receiving sensitive information over the internet so we want to provide security of text/images or messages, we are sending with over the receiver. The main problem in this state of affairs is the fact that, no matter which way you look at it, ultimately, you have to offer users a link to the downloadable file. Once an important person has that link, they can suggest it to their friends and colleagues, who then simply outwit all of your security features and download the file directly. None of the security features you put in place are worth anything if a user knows that final link to the downloadable file itself. Writing secure code and knowing how the system/environment impacts for security measures is important to designing secure software. Solutions extend beyond writing secure software; secure software involves designing a system that will likely interact with users, and legacy systems to meet some objectives.

II. PROBLEM STATEMENT

Providing security to the client in a Computer Network prevailing now a days is taken as the problem domain for the current work.

III. LITERATURE SURVEY

There are various security based techniques available to rupture the majority of the encryption algorithms at one point of time like linear cryptanalysis, n-gram analysis, brute force attack, man in the middle attack etc. [Berouz Forouzan (2013)]. Furthermore in recent past, there was some famous algorithms have been developed like RSA, DES or the AES. These algorithms look secure. But these algorithms have a significant drawback that, they are not able to eliminate the repetition of data values in the cipher text which is called as patterns [G. Usha Devi, Ipsita Rana, Sutanu Nandi, (2012)]. Besides these some multilevel encryption system have been developed using the existing cryptographic algorithms to provide more security [Sairam Natarajan, Manikandan Ganesan, Krishnan Ganesan (2011)]. But the disadvantage of this kind of multilevel system is that it is relatively slow compared to other cryptographic algorithms because of multiple levels and multiple algorithms. In recent past some multilevel encryptions using graceful code have also been developed. They eliminate the patterns [G. Usha Devi, Ipsita Rana, Sutanu Nandi, (2012)] but the disadvantage is that one character is encrypted into fixed number of data values [Sairam Natarajan, Manikandan Ganesan, Krishnan Ganesan (2011)]. So they can be vulnerable to the attackers.

C. Sanchez-Avila et.al analyzed the structure and design of Rijndael cipher (new AES), remarking its main advantages and limitations, as well **as** its similarities and dissimilarities with DES and T-DES. Finally, a performance comparison among new AES, DES and T-DES for different microcontrollers has been carried out, showing that new AES have a computer cost of the same order than the one needed by T-DES [C. Sanchez-Avila et.al]. A. Murat Fiskiran et.al showed some cryptographic algorithms that have properties that make them suitable for use in constrained environments like mobile information appliances, where computing resources and power availability are limited characterization of the instructions executed by these algorithms, and demonstration that a simple processor is sufficient. Also a set of public key, symmetric key and hash algorithms suitable for such environments and studied their workload characteristics. It also describes the instructions needed by different algos: Diffie Hellman key exchange, AES, Hash. All are compared using simple RISC style processor with ALU and shifter and workload characteristics can be determined [Murat Fiskiran, Ruby B. Lee].

Suhaila Orner et. al discussed the security and attack aspects of cryptographic techniques and also discussed the dominant issues of security and various attacks. Finally, bench marked some well-known modern cryptographic algorithms in search for the best compromise in security. In this paper, CrypTool was used as a simulator to conduct the experiments and to get the result. Only alphanumeric and special characters are used for analysis of cryptographic techniques. These specifications are selected in option menu of the CrypTool and visual results are set in window option of the CrypTool. For the input plaintext, around 25-sample text are taken and encrypted with various algorithms. The output of above plaintext is cipher text, analyzed with analysis option in CrypTool. Some of the cryptographic algorithms are implemented in C, and their output is taken as cipher text, which is then copied in some text file and that text file is used for the analysis with CrypTool [Suhaila Orner Sharif, S.P. Mansoor]. In [15] Vaibhav et. al. proposed a Model which can be used to detect Intrusion made in a Cloud by the use IDS which is proposed to be built in Artificial Neural Network framework. In [16] Vaibhav et. al. proposed the use of Data mining landscape for detecting frauds in digital data. In [17] Vaibhav Kant Singh and Amrendra Kumar Singh proposed a dual level digital watermarking system for Images.

IV. PROPOSED WORK

Sender is supposed to send information in the network this may be by means of a text file, image file or message through Emails. The data that is transferred over a network may contain data that is Grey colored or colored data or a combination of both. From security point of view we may change the coloring of data present in the document. The Data file Text/Image or message is broken into packets before transmitting over the network. For example: Suppose we have one file the size of which in disk is 80KB. Now, suppose we want to transfer this file over network and the offered packet size is 1KB of Data per packet excluding the header. Therefore there will be generation of 80 packets which will be transferred over the Network. The packets containing the data have information about the colors present in the document .The RGB intensity values are associated with every packet. Above type of data we send to the third party for the providing security. When one packet passes from sender machine to receiver machine; the transferred packets will not be allowed to open before the receiver received packet information of RGB from the third party. Whenever third party receives the RGB data with intensity values from the sender machine it passes this data to the receiver machine. In receiver end first receive the RGB intensities value and the original data in the form of packets. (The RGB color model is an additive color model in which red, green and blue lights are added in a different ways. To verify the authenticity, the first step is to assign a unique color for each receiver. By using appropriate combination of red, green and blue lights various colors can be represented). After extracting the text we matched the both information, if the information are not matched then system / application will not allowed to open the data. If intruders arrived or attack in between sender and receiver then sender text not useful for intruders because they have no key information of RGB intensities values (that data provided by the third party).If our applications are successfully run, than receiver received data from sender machine and from third party. If both information are similar than our application will do work and match both messages. Finally, Received data are fully secured and open in our original format. Otherwise, if both data packet one from sender machine and one from third party message will be not matched then our application will not open the original data. There is no defining blue print on what is the best language to learn. There for we would like to prefer .NET / MATLAB too good alternatives that we think are a good language to learn in computer or network security.

The Proposed model is Explained by means of the Figures 1, Figure 2, Figure 3, Figure 4, Figure 5, Figure 6 and Figure 7. The Figures 1, Figure 2, Figure 3, Figure 4 and Figure 5 shows the normal mode of operation exhibited in the Computer Network. In the proposed model we will add a new trusted third party which will enable only authentic sender to have its information destined. The methodology adopted by the model is already explained in this section above.

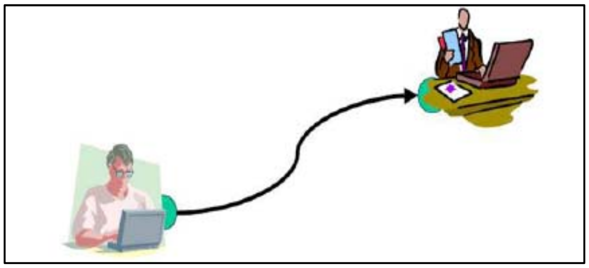

Figure1:-Information Transferring from Sender Machine to Receiver Machine.

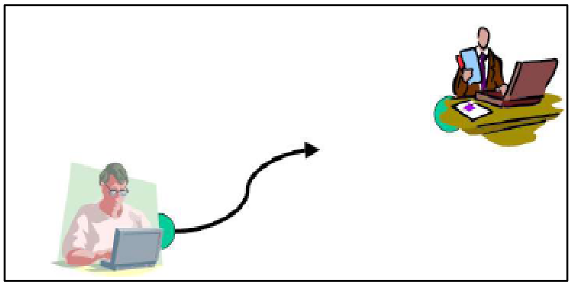

Figure2:-Intended Information Transfer from sender machine to receiver machine but break in the transfer due to interruption

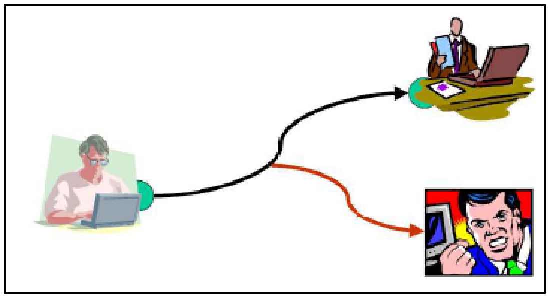

Figure3:-Information Transfer from Sender to Receiver being visualized by an Intruder (Interception Made)

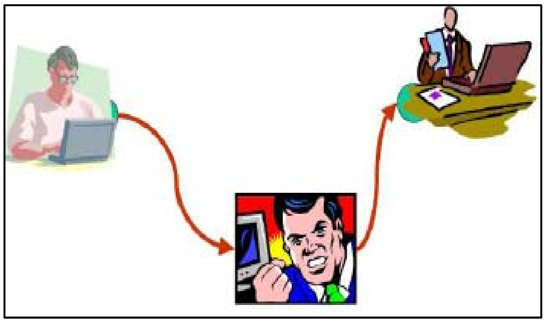

Figure4:-Information being modified by the Intruder (If desired)

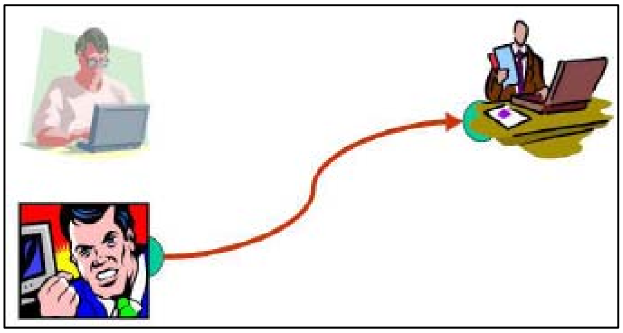

Figure5:-Intruder taking full control of the Data being transmitted to the cloud (Fabrication Enabled)

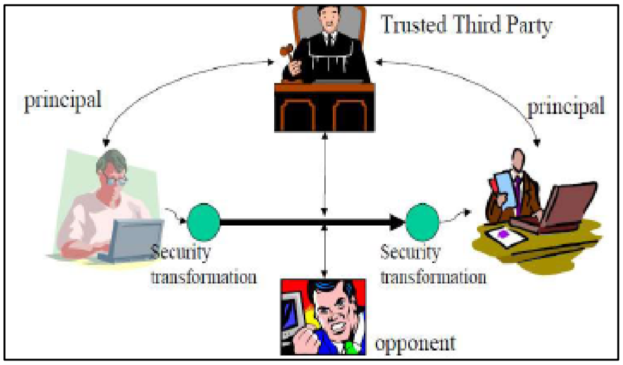

Figure6:- Proposed Network Security Model with Third Trusted Party

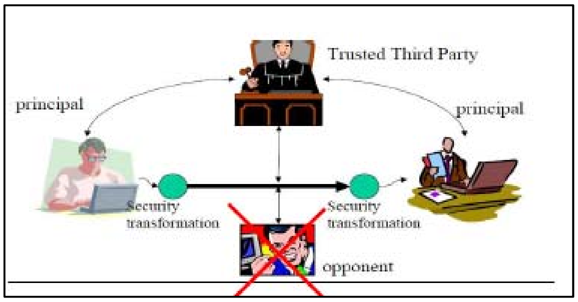

Figure7:-Proposed Model breaking the threat which may be caused in a normal Computer Network

V. CONCLUSION

The designed system provides the security for packet transfer. We give the prime importance for the data security in email system which is widely used in day to day life. Thus, we address the problem of security regarding unauthentic headers in the email. For this, we had used a textual password using color combination of RGB model and for encryption and decryption of message content we had used megamall cryptography which is efficient in terms of software and hardware implementation. As our proposed scheme uses advanced authentication technique and is well adapted to any possible future technology. Sender is supposed to send information in the network.

REFERENCES

[1] A. Kahate, Cryptography and Network Security, Tata McGraw Hill Publications.

[2] S.P. Deepa, S. Kannimuthu and V. Keerthika, “Security using colors and Armstrong Numbers,” Proceeding of the National Conference on Innovation in Emerging Technology, 2011.

[3] S.A. Saoji, N.B. Agarwal, M.B. Bokil and A.V. Gasavi, “Securing E-mails in XML format using colors and Armstrong numbers,” International Journal of Scientific & Engineering Research, 2013.

[4] G.U. Devi, I. Rana and S. Nandi,” Multilevel Encryption System using Graceful Codes,” International Journal of Advanced Research in Computer Science and Software Engineering, 2012.

[5] B. Forouzan, Cryptography and Network Security, 2nd Edition, TMH.

[6] B.R. Bandawane, M.M. Gangadhar and B.D. Kumbhar, “Data security using graphical password and AES algorithm for E-mail system,” IJEDR, 2014.

[7] A. Shetty, K.S. Shravya and K. Krithika, “A review on Asymmetric Cryptography-RSA and ELGamal algorithm,” International Journal of Innovative Research in Computer and Communication Engineering, 2014.

[8] S. Natarajan, M. Ganesan and K. Ganesan, “A Novel Appraoach for Data Security Enhancement using Multilevel Encryption Scheme,” International Journal of Computer Science and Information Technologies, vol 2, issue 1, pp. 469-473, 2011

[9] L. Liao and J. Schwenk,”Secure E-mails in XML format using Web Services,” Fifth European Conference on Web Services.

[10]N. Godbole, Information Systems Security, Wiley India Pvt. Limited.

[11]G. Shroff, Enterprise Cloud Computing, Cambridge.

[12]M. Fiskiran and R.B. Lee, “Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments,” IEEE International Workshop on Workload Characterization, 2002.

[13]S.O. Sharif and S.P. Mansoor, “Performance analysis of stream and block cipher algorithms,” 3rd International Conference on Advanced Computing Theory and Engineering, (ICACTE), 2010.

[14]S. Avila and C.S. Reillol,”The Rijndael block cipher (AES proposal): A Comparison with DES”, IEEE 35th International Conference on Security Technology, 2001.

[15]V.K. Singh and D.K. Singh, “Proposing BPN based IDS for security in Cloud,” Proceeding of 10th International Conference on Instrumentation, Electrical and Electronics Engineering (ICIEEE 2015) & 10th International Conference on Cloud Computing Computer Science and Advances In Information Technology (ICCCCIT 2015), TROI India, pp. 1-7, 20 September Delhi, 2015.

[16]V.K. Singh, V. Dubey and A.K. Singh, “Proposing Data Mining as an Efficient Technique for Solving Frauds in Digital data,” Proceeding of 1st International Conference on Intelligent Information Systems and Management, IISM’10, RVS College of Engineering and Technology, Coimbatore, Tamilnadu, pp. 1-4, June, 2010.

[17] V.K. Singh and A.K. Singh, “Dual Level Digital Watermarking for Images,” Proceeding of International Conference on Methods and Models in Sciences and Technology (ICM2ST-10), Published by American Institute of Physics(AIP), pp. 284-287, Chandigarh, 2010.