International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

A Survey on Encryption Using Dynamic Key Generation

Naik Riddhi[1],Prof. Nikunj Gamit[2]

[1]*Computer Engineering, CGPIT, Uka Tarsadia University Bardoli, Surat,riddhi262@gmail.com*
[2]*Computer Engineering, CGPIT, Uka Tarsadia University Bardoli, Surat,nikunj.gamit@utu.ac.in*

Abstract—Security is an important issue in communication and storage of information, and encryption is one of the ways to ensure security. Many existing algorithm for encrypting and decrypting the user messages are available all over the world. Security often depends on keeping the key secret. Cracking key used for encryption must be very difficult task. There have been many attacks or approach designed to crack the key for well-known algorithms. One way to make a system more secure is to change the key on periodic basis. This study concentrates on various techniques for dynamic key generation using the color image for security.

Keywords-Encryption, Dynamic key Generation, Color Image, Decryption, LSB

I. INTRODUCTION

Our routine life is carrying an essential dependability on internet technologies and their expertise in various activities. It has advantages and disadvantages. The growing prospects of modem communications need the exceptional means of security especially in computer network communication. The network security is gaining importance as the data being exchanged on the internet increases. As the data exchange in electronic way is rapidly increasing, it is also equally important to protect the confidentiality of data from unauthorized access. The data exchange can be text, image, audio, video etc. Each type of data has its own features different techniques are used to protect confidential data from unauthorized access. The cryptography has been proposed to ensure the confidentiality and authenticity of the message. The encryption key must be long. Yet, it is difficult to remember it and even storing the key in a database or in a file may be insecure. In addition the protection of the confidentiality of encryption keys is one of the important issues to be dealt with. This issue can be efficiently solved through generating the key before starting the process of encryption and decryption, rather than storing it. The main objective of this study is to increase security in communication by encrypting the information using a key that is created through using an image [3]. Color images are used for key generation which is based on different session. Instead of storing and remembering the secret key we can store the images in the database [2].

II. TECHNIQUES ON DYNAMIC KEY GENERATION

Progress of communication technologies in contemporary times has resulted in huge quantities of digital data in the publicly shared media. The data exchanged can be text, image, audio, video etc. Each type of data has its own features different techniques are used to protect confidential image data from unauthorized access.

2.1.Graphical Password Generation Using Image

Graphical password is one of the alternative solutions to alphanumeric password as itis very tedious process to remember alphanumeric password. One of the major reasons behind this method is

according to psychological studies human mind can easily remember images than alphabets or digits. Here one algorithm is explained which is based on selection of username and images as a password. By this paper we are trying to give set of images on the basis of alphabet series position of characters in username. In this method there are main four steps for key or password generation for login.

2.1.1. Registration

In the first step for registration user have to pass through authentication process. In that on the basis of username, process will be started at the server-side. Set of images which will be provided to user are based on username [1].

2.1.2. Calculation on the Basis of Username

In the second step calculation on the basis of username is done. At the server-side positionof usernames alphabet in alphabet series will be calculated. Then addition of all the positions is done. First digit of that sum will be considered for further calculations [1].

2.1.3. Assigning Set of Images

Third step is assigning set of images. There are total 26 alphabets present in alphabetseries. We know that any two digit number can start with number 1-9. Server has already made set of images. Set of images will be assigned according to result of calculation which server has got at the second step. Means if first digit is 1, then set assigned to it will set of A. If first digit is 2, then set assigned to it will be B [1].

2.1.4. Selection of Password

Last step is selection of password. In this complete password is divided in two sections first is based on user selection, second is based on server provided sets of images. For user selection, from given set of images user has to select two images as the password. From sever end two images will be provided to user so as to form complete password [1].

In this method selectable images are used, user can have more number of images on each page and among this entire password is selected. Images are different for each case, so if hackers try to match the each combination to find the correct password it will take millions of year. But drawback of is method is that it cannot be used for encryption process and through this method we can generate only one password.

2.2.Randomized Cryptographic Key Generation Using Image

Other approach for randomized cryptographic key generation using image is proposed.There are main four phases in this system which are image database, key generation, encryption and decryption.

2.2.1. Image Database

In first phase twenty four images are used on hourly basis. The images are color image. Once the sender and the receiver are ready for communication access are given of the image data base. Only authorized sender and receiver can access the image database.

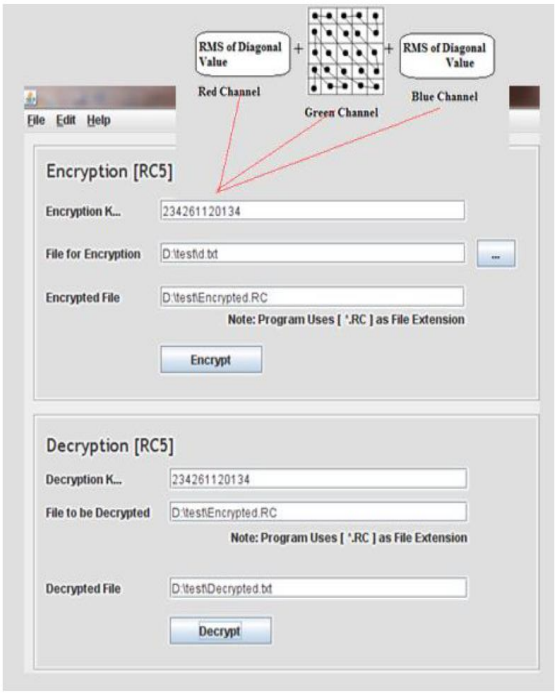

Figure 1. RC5 Encryption using dynamic key generation [2]

2.2.2. Key Generation

Second phase is key generation based on the image stored in the database. Consider the pixel value of an image and extract one channel (R/G/B) at a time. It can be either a red channel or green channel or blue channel. The key is generated based on the following steps. First red channel is extracted from image and RMS is calculated of diagonal pixel and the generated RMS value is considered as a part of the key and it is stored in a variable. After that green channel is extracted and sum of all the pixel values in a zigzag manner is calculated and stored in one variable. After that blue channel is extracted form image and RMS is calculated of diagonal pixel. After that the value got using the red channel is appended with the value got using the green channel and the blue channel value is also appended to generate the key [2].

2.2.3. Encryption and Decryption

Encryption and decryption is performed using RC5 algorithm and key which is generatedthrough key generation algorithm [2].

This system is secured against the man in middle attack, compromised key attack and system attack. This system focuses on generating key based on images. The generated key need not have to be stored. It can be generated anywhere using the image and the session. To generate the original message from the cipher text one has to know the session on which the encryption is done, image considered for encryption, RGB values taken and processed for key generation. There by it creates a complex system for cracking and an easy way to implement.

2.3.Cryptography Method Based on Image for Key Generation

There is one other approach which is used for image encryption using dynamic key generation algorithm. In this approach key is generated using image. This study proposes a method for encrypting the sender's messages using new algorithm with a secret key which is generated from using color image and the difference in the LSB of the image pixels. This key will be used for encrypting and decrypting the messages which are transmitted between two sides. The length of the

key varies according to the size of the message as it varies in every session according to the session type. There are main four phases in this method which are database creation, key generation, encryption and decryption.

2.3.1. Database Creation

In the first phase which is database creation, database of color image is created whichare used for key generation process. In case of using hourly session, the database should contain 24 images; otherwise, it should contain 7 images for the daily session. Both the sender and the receiver should use the same database of images as the names of the images should be the same in both sides [3].

2.3.2. Key Generation

The other phase is key generation phase in which key are generated from the images for encryption and decryption process. In this process first of all value of K and N is extracted. N is the length of message and K is any even random number between 2 and N. After that color image is selected from the database according to session type and current date or time and any one channel is extracted from that image. Extracted channel is converted into binary number and LSB of that number is calculated and stored it in one array. Now each bit of generated array is scanned and two bits are stored in other array whose absolute different is one. Through this process new array of N*K is generated which is key [3].

2.3.3. Encryption and Decryption

After generation of key third phase is encryption phase. In this phase message is scanned and binary conversion of that message is done. Through binary conversion one array is generated of N*N size where N is length of message. After that XOR operation is performed between key array and message array and result of this operation is stored in other array which is encrypted array. This encrypted array is converted into character form which is cipher text. After encryption process cipher text is passes to receiver and reverse process of encryption is perform at receiver side to get the original message again using the same key which is generated in key generation phase and used for encryption process [3].

These methods create more complexity to creak or guess the keys by using the cryptanalysis technique. To break this algorithm we need to know the image database, color image channel, the key value and the session type.

2.4.Session Key Generation Using Fingerprint

This system uses two algorithms known as Bio-Metric Encryption Algorithm (BEA), Minutiae Extraction Algorithm (MEA). It uses Multi Bio-metric features for authentication purpose. And also this system dynamically generates a new Session Key for each transaction. The main objective of the this system is to provide secure transaction and to restrict the Online attacks such as Dictionary Attack, Brute force attacks, Masquerade, Modification of messages, IP Spoofing etc. using some authentication techniques [4]. In biometric cryptosystems, a cryptographic key is generated from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication. Fingerprint patterns are stable throughout person's life time. In the proposed system the user must give both Username and Password for authentication purpose. This system uses Multi Biometric features such as both left and right fingerprints of the user. Cryptography key is generated from a left and a right fingerprint is combined with the key generated from Users password. This Session key is encrypted using Some Cryptographic Algorithm with some key which is already shared by sender and Receiver. This Session key will be decrypted using the same key in receiver side [4].In this main three phases are considered which are dynamic session key generation, encryption and decryption.

2.4.1. Key generation

In dynamic session key generation main five steps are performed. These main steps are shown in figure 2.

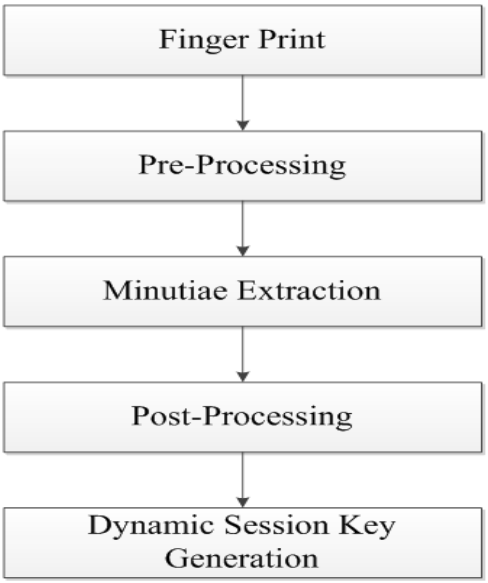

Figure2. Steps for Key Generation [4]

First step is fingerprint in which image of fingerprint is extracted [4]. After that preprocessing operations are performed on this image. In preprocessing first of all image enhancement is done where the Fingerprint enhancement is anticipated to improve the contrast between ridges and valleys and reduce noises in the fingerprint images. Second operation in preprocessing is binarization. Binarization is the process that translates a grey level image into a binary image. This enhances the contrast between the ridges and valleys in a fingerprint image, and consequently makes it possible the extraction of minutiae. Third process of preprocessing is thinning which is a morphological operation that is used to remove selected foreground pixels from binary images, somewhat like erosion or opening. After thinning fourth process is ROI extraction. In the fingerprint image, the region of interest (ROI) is the area of an image, which is importance for extraction of minutiae points. For ROI extraction two Morphological operations OPEN and CLOSE are used. The OPEN operation can expand images and remove peaks introduced by backround noise The CLOSE operation can shrink images and eliminate small variations [4].

After preprocessing minutiae extraction is performed in which Fingerprint is distinguished with the help of minutiae, which are the some abnormal points on the ridges [4]. After this last step post processing is performed. The minutiae points obtained in the above step may contain many spurious minutiae. This may occur due to the presence of ridge breaks in the given figure itself which could not be improved even after enhancement. This results in false minutiae points which need to be removed. These unwanted minutiae points are removed in the post-processing stage. So to keep the recognition system consistent these false minutiae need to be remove. This process helps in removing false minutiae [4].

2.4.2. Encryption and Decryption

After key generation encryption and decryption phases are performed. Biometric Encryption algorithm provides a mechanism for the linking and retrieval of a binary key of the user's password with the Dynamic Session key from the user's fingerprint [4]. This algorithm generates the different key at each time. These values are encrypted using Blow fish algorithm. This increases the secrecy of

key. Before the encryption process the sender and receiver must share their secret using RSA key exchange algorithm [4].
This system dynamically generates a new Session Key for each transaction. So the proposed system will protect Data Confidentiality, Data Integrity, Authentication, Availability, Access control of information over the network.

III. SUMMARY

In above sections some techniques are discussed for security of data using key generation process. Comparative analysis of those systems is as shown in table 1.

Table 1. Summary

No	Techniques	Advantages	Disadvantages
1.	Graphical password generation using image	1)More number of images are used 2) More time will required for combination of images 3) Graphical password provide more memorable password	1) Access can be given if anyone knows sequence with user name 2) Dynamic key cannot be generated
2.	Randomized cryptographic key generation using image	1)Secure against man-in-middle, compromised key and system attacks 2) Less complexity 3) Variable length key 4) Not necessary to remember the key	1) Key can be guessed if database is access by unauthorized person 2) RC5 is used for encryption and decryption algorithm which is very time consuming
3.	Cryptography method based on image for key generation	1)Key gets change with period of time 2) Not affected by brute force attack 3) Key length varies according to input text	1) Value of K is assumed 2) More assumption are made 3) In encryption and decryption process unnecessary computation are performed
4.	Session key generation using fingerprint	1)Dynamic key can be generated 2) Protect data confidentiality, data integrity, authentication, availability and access control over network	1) Key is shared among sender and receiver

CONCLUSION

The communication technologies have major impact in this world hence to ensure security while transferring of information is important. In this study deep analysis is made on dynamic key generation techniques based on color images, fingerprint and genetic algorithm. The generated keys need not have to be stored. It can be generated anywhere using the image and the session base.Encryption and Decryption processes are based on session on which the process is done and key

generated through key generation.These provide more security against man-in-middle attack and brute force attack.

REFERENCES

[1] ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare,"Graphical Password Authentication: Cloud securing scheme", International Conference on Electronic Systems, Signal Processing and Computing Technologies,2014 IEEE.

[2] Priyanka.M, Lalitha Kumari.R, Lizyorance.C, John Singh. K,"A New RandomizedCryptographic Key Generation Using Image", International Journal of Engineering Science and Innovative Technology (IJESIT), ISSN: 2319-5967, ISO 9001:2008 Certified Volume 2, Issue 6, November 2013.

[3] Taw_q S.Barhoom, Zakaria M.Abusilimiyeh,"A Novel Cryptography Method Basedon Image for Key Generation", Proceedings on the Palestinian International Conference on Information and Communication Technology, 2013 IEEE, pp: 71-76.

[4] T.Mekala, N.Madhu Suganya,"Secure Transaction Using Dynamic Session Key", International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue 4, March 2013.

[5] Article Neerav Bhatt (excepting attributed sources).

