FILE ENCRYPTION AND OTP: A COMPLETE REVIEW

Anjali[1], Shashi Sharma[2]
[1]M.Tech Scholar, [2]Assistant Professor
Computer Science Department, Jaipur Institute of Technology.

Abstract: In the case of the networking the big issue is sharing the file securely and it is often desired that the content of the files cannot be interpreted by the intruder. Thus in this paper, we review the technologies in the file encryption and various type of password concepts in securing the data from the intruders.

Keywords: File Encryption, Data Encryption, Passwords.

I. INTRODUCTION

File encryption: Cryptography is the training and investigation of techniques for secure communication within the sight of outsiders. All the more by and large, it is about developing and examining conventions that conquer the impact of enemies and which are identified with different viewpoints in information security, for example, data classification, data uprightness, confirmation, and non-revocation.

Cryptography before the advanced age was adequately synonymous with encryption, the change of information from a clear state to evident rubbish. The originator of an encrypted message shared the deciphering system expected to recoup the first information just with proposed beneficiaries, accordingly blocking undesirable people to do likewise.

Since World War I and the appearance of the PC, the methods used to do cryptology have turned out to be progressively mind boggling and its application more across the board. Cryptography incorporates the accompanying procedure:

Encryption and Decryption;
It is the way toward changing over normal information (called plaintext) into incomprehensible text (called ciphertext). Decryption is the turn around, at the end of the day, moving from the muddled ciphertext back to plaintext. A figure is a couple of calculations that make the encryption and the turning around decryption.

The itemized operation of a figure is controlled both by the calculation and in each occurrence by a "key". This is a mystery (in a perfect world known just to the communicants), more often than not a short series of characters, which is expected to unscramble the ciphertext.

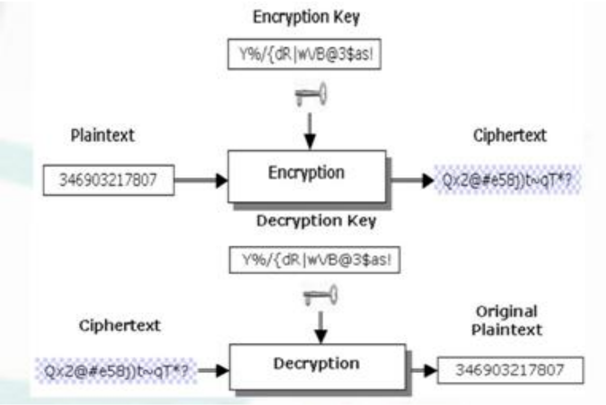

Figure 1: Process of Encryption and Decryption

OTP: Security is a noteworthy concern today in all segments, for example, banks, administrative applications, military association, instructive organizations, and so forth. Government associations are setting standards, passing laws and forcing associations and organizations to conform to these standards with rebelliousness being met with far reaching outcomes. There are a few issues with regards to security worries in these various and changing ventures with one normal feeble connection being passwords.

The fast development in the number of online administrations prompts an expanding number of various advanced personalities every client needs to oversee. Be that as it may, passwords are maybe the most widely recognized sort of qualification utilized today [5]. To stay away from the dreary assignment of recalling troublesome passwords, clients often carry on less securely by utilizing low entropy and feeble passwords.

Most systems today depend on static passwords to check the client's personality. In any case, such passwords accompanied significant administration security concerns. Clients tend to utilize simple to-figure passwords, utilize a similar secret word in numerous records or store them on their machines, and so on. Besides, programmers have the alternative of utilizing numerous techniques to take passwords, for example, bear surfing, snooping, sniffing, speculating, and so forth. In addition passwords can be composed down, forgotten and stolen, speculated purposely being advised to other individuals.

II. TECHNIQUES OF FILE ENCRYPTION AND DECRYPTION

Following are the modern field of cryptography:

a) Symmetric-Key Cryptography

Symmetric-key cryptography alludes to encryption methods in which both the sender and beneficiary offer a similar key. Symmetric key figures are actualized as either piece figures or stream figures. A square figure enciphers contribution to pieces of plaintext rather than singular characters, the information form utilized by a stream figure. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are square figure outlines which have been assigned cryptography standards by the US government.

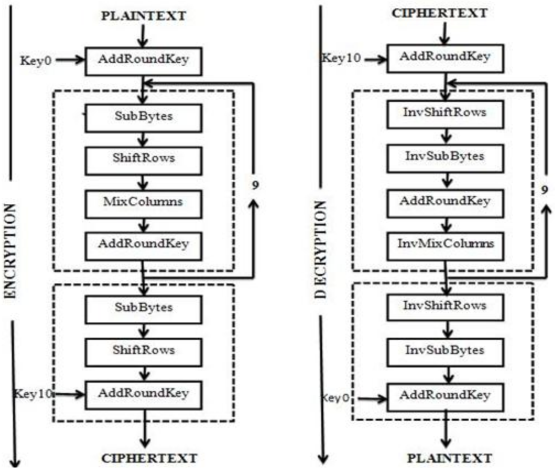

Fig. 2AES Encryption and Decryption

b) Public-Key Cryptography

Symmetric-key cryptosystems utilize a similar key for encryption and decryption of a message, however a message or gathering of messages may have an unexpected key in comparison to others. A critical drawback of symmetric figures is the key administration important to utilize them securely. Each unmistakable match of conveying parties must, in a perfect world, share an alternate key, and maybe each ciphertext traded too. The number of keys required increments as the square of the number of system individuals, which rapidly requires complex key administration plans to keep them all steady and mystery. Diffie and Hellman's publication started far reaching scholastic efforts in finding a handy public-key encryption system. This race was at long last won in 1978 by Ronald Rivest, Adi Shamir, and Len Adleman, whose arrangement has since turned out to be known as the RSA calculation.

c) Cryptanalysis

The objective of cryptanalysis is to discover some shortcoming or insecurity in a cryptographic plan, therefore allowing its subversion or avoidance. It is a typical misguided judgment that each encryption strategy can be broken. Regarding his WWII work at Bell Labs, Claude Shannon demonstrated that the one-time cushion figure is unbreakable, given the key material is really random, never reused, kept mystery from every single conceivable aggressor, and of equivalent or more noteworthy length than the message. Most figures, aside from the one-time cushion, can be broken with enough computational effort by beast force assault, yet the measure of effort required might be exponentially reliant on the key size, when contrasted with the effort expected to make utilization of the figure

III. OTP SYSTEM DESIGN AND WORKING

we propose a PC based software token. This should supplant existing equipment token gadgets. The System includes era of Secured OTP utilizing Cryptographic calculation and delivering it to client's mobile as SMS or client can ready to make his own OTP utilizing cell phone and approving the OTP utilizing same Cryptographic calculation. The proposed system is secured and comprises of two sections: (1) the server software, (2) the customer software: Client application on PC for exchange and android application on cell phone for making OTP.

3.1 Otp Algorithm:

keeping in mind the end goal to secure the system, the produced OTP must be difficult to figure, recover, or follow by programmers. Therefore, it is essential to build up a secure OTP creating calculation. A few components can be utilized by the OTP calculation to produce a hard to-figure watchword. Clients appear to utilize basic variables, for example, their mobile number and a PIN for administrations, for example, approving mobile miniaturized scale installments, so we propose a Secured Cryptographic calculation.

The [5] extraordinary OTP is created by the mobile application offline, without connecting to the server. The mobile telephone will utilize some remarkable information keeping in mind the end goal to produce the watchword. The server will utilize a similar special information and approve the OTP. All together for the system to be secure, the one of a kind OTP must be difficult to foresee by programmers. The accompanying elements will be utilized to generate the OTP:

IMSI number: The term stands for International Mobile Subscriber Identity which is an extraordinary number related with all GSM and Universal Mobile Telecommunications System (UMTS) arrange mobile telephone clients. It is put away in the (SIM) card in the mobile telephone. This number will likewise be put away in the server's database for every customer.

ATM PIN: Needed for checking the realness of the customer. On the off chance that the telephone is stolen, a substantial OTP can't be produced without knowing the client's PIN. The PIN isn't put away in the telephone's memory. It is just being utilized just to produce the OTP and obliterated quickly after that.

Timestamp: Used to produce one of a kind OTP, legitimate for a short measure of time. The timestamp on the telephone must be synchronized with the one from the server.

DOB: Date of birth of client whose going to utilize the application.

Username: Username of client given by bank

3.2 Methods for delivering OTP:

Text Messaging:

A continuous innovation utilized for the conveyance of OTPs is text messaging. Since text messaging is an ever-show communication station, and is straightforwardly accessible in every mobile handset and, through text-to-discourse transformation, to any landline phone or mobile handset, text messaging is probably going to achieve all clients with a minimal effort to execute. OTP over text messaging may be encrypted utilizing an A5/x standard, which some hacking bunches report can be successfully unscrambled inside minutes or seconds, or the OTP over SMS won't not be encrypted by one's specialist organization at all[9]. The mobile telephone administrator turns into a piece of the put stock in chain. On account of wandering, more than one mobile telephone administrator must be trusted. Utilizing this data may build a man-in-the-center attack.

Mobile phones:

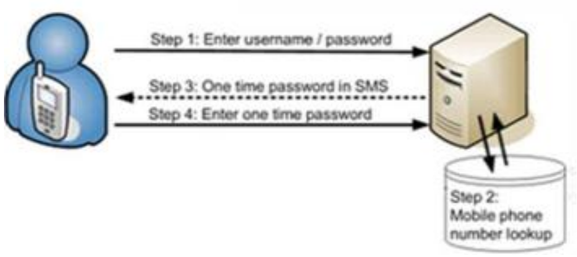
Step 1: Enter username / password
Step 3: One time password in SMS
Step 4: Enter one time password
Step 2: Mobile phone number lookup

Figure 1: Steps to get OTP on Mobile Phone

A mobile telephone minimizes expenses as a huge number of individuals utilize mobile telephone for different reasons other than creating OTPs. Mobile telephones furthermore bolster any number of tokens inside one establishment of the application [9], and from one gadget client will be confirmed to various assets. Demonstrate particular applications as per client's mobile telephone are likewise accessible.

Web based methods:

Authentication offers different web based methods for delivering one time passwords without the utilization of hardware tokens. Such techniques rely on upon client's capacity to perceive pre-picked categories from a randomly produced accumulation of pictures. While enrolling on a website, the client picks a few categories of pictures, for example, creatures, autos, VIPs and blooms. At whatever point client would login the website they are given a randomly produced lattice of picalphanumeric character overlaid on it [9]. The client searches for pictures that fit their pre-picked categories and enters the related alphanumeric characters [9] to form one time password.

Hardcopy:

In a few nations for web based keeping money, the bank sends client a rundown of OTPs that are imprinted on paper. Different banks send plastic cards with real OTPs secured by a layer that the client needs to scratch off to unveil a numbered OTP. To do online exchange, the client is required to enter a particular OTP from that rundown. Some system ask for numbered OTPs consecutively, others pseurandomly pick an OTP to be entered.

IV. ATTACKS

In the Phishing Attack [6][7], the assailant achieves the client information, by going about as a capable individual. Phishers endeavor to falsely secure delicate information, for example, passwords and charge card subtle elements, by taking on the appearance of a dependable individual or business in an electronic communication. For instance, a phisher can set up a fake website and then send a few messages to potential casualties to induce them to get to the fake website. Along these lines, the phisher can without much of a stretch get an unmistakable text of the casualty's password. Phishing attacks have been ended up being extremely compelling.

In the Password Stealing Program Attack, software codes are utilized to accomplish the password. The Key Logger Program and Trojan Redirectors are case for password stealing program.

In the Key Logger [8], the software that will be introduced on the system and that software records every one of the exercises done on the key board are recorded. At whatever point the client confides in the outsider system, that software might be introduced on the system. This kind of software not shown on the errand director. From the recorded key, the assailant gets the password inside a brief timeframe and less effort. The Trojan Redirectors uses to divert the system into attacker favored area.

In Shoulder-Surfing Attack, the camera is settled to screen every one of the exercises of the client. For this reason, the shrouded cameras are ordinarily utilized by the assailant. Shoulder surfing is especially powerful in swarmed places since it is generally simple to watch somebody as they:

Fill out a form:

Enter their PIN at a computerized teller machine or a POS terminal

Utilize a phone card at a public payphone

Enter a password at a digital bistro, public and college libraries, or airplane terminal booths

Enter a code for a leased locker in a public place, for example, a swimming pool or air terminal

Shoulder surfing should likewise be possible at a separation utilizing binoculars or other vision-upgrading gadgets. Reasonable, small shut circuit TV cameras can be hidden in roofs, dividers or apparatuses to watch data passage. To avert bear surfing, it is encouraged to shield printed material or the keypad from see by utilizing one's body or measuring one's hand. The attacker may utilize any of the assaulting system for acquiring the password without learning of the client.

The attacker does any false exercises utilizing the password and in saving money exchange they may exchange client's add up to their record. It might harm the client's close to home life. To stay away from password stealing, pick the password as an extremely solid one, and it ought to be changed every now and again and ought to be effortlessly vital by the client. One time password component, virtual keypad, graphical password and biometric based authentications are recommended as a therapeutic measure to beat the previously mentioned attacks.

Password Stealing Attacks Choosing An Appropriate Password

By following rules for choice of a password, the danger of a password being traded off through speculating or breaking is significantly diminished [4][5]. The level of password quality required depends, to a limited extent, on how simple it is for an aggressor to present numerous speculations.

While a few systems constrain the number of times that a client can enter a wrong password before a deferral is forced or the record is solidified, different systems permit for all intents and purposes boundless login endeavors. An assailant can attempt passwords by speculating normally utilized ones based on a client's name and other individual information. Regular rules for fitting password determination are:

Make passwords as far as might be feasible, as longer passwords are harder to figure.

Use however many diverse characters, numbers and images as could reasonably be expected to make it more tough to figure.

Try not to utilize normal lexicon words, as they are less demanding to figure than random characters.

Try not to utilize individual information, since it is certainly speculated.

Change passwords all the time to limit the threat of bargained passwords.

While following such rules can decrease the possibility that a password will be speculated and therefore traded off, a more grounded support for following these practices is to diminish the change that password breaking software will bargain a password.

V. CONCLUSION

The remarkable components of the proposed asymmetric picture encryption plan can be condensed as: (a) Lossless encryption of picture. (b) Less computational intricacy. (c) Convenient acknowledgment. (d) Choosing a reasonable size of network as per the measure of picture. (e) Encryption/decryption conspire utilizes whole number math and rationale operations. Both shading and dark and white picture of any size spared in labeled picture file format (TIF) can be encrypted and decoded utilizing blowfish calculation. MREA calculation is utilized to scramble files and transmit encrypted files to flip side where it is unscrambled. Principle highlight of this strategy is that it fulfills the properties of Confusion and dispersion and additionally has an ideal figure of encryption key makes decryption outlandish Single component authentication, e.g. passwords, is never again thought to be secure in the web and managing an account world. Simple to-figure passwords, for example, names and age, are effortlessly found via mechanized password-gathering programs. Two element authentication methods have as of late been acquainted with address the issues of organizations for giving more grounded authentication alternatives to its clients. As a rule, a hardware token is given to every client for each record. The expanding number of conveyed tokens and the cost the assembling and keeping up them is troublesome for both the customer and organization. Numerous customers convey a mobile telephone now consistently. An option is to introduce all the software tokens on the mobile telephone, which decreases the assembling costs and the number of gadgets conveyed by the customer. The proposed work concentrates on the execution of two-consider authentication methods utilizing mobile telephones. It gives an outline of the different parts of the system and the abilities of the system. The proposed system has two alternative of running, either utilizing a free and quick association less technique or a marginally more costly SMS based strategy. Both methods have been effectively executed and tried, and appeared to be robust and secure. The system has a few components that make it hard to hack.

REFERENCES

[1] Amrita Sahu, Yogesh Bahendwar, Swati Verma, Prateek Verma, "Proposed Method of Cryptographic Key Generation for Securing Digital Image", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[2] Pavel Berkhin, A Survey of Clustering Data Mining Techniques, pp.25-71, 2002.

[3] Han J. and Kamber M., Data Mining: Concepts and Techniques, 2nd ed., San Francisco, Morgan Kauffmann Publishers,2001.

[4] S. Furnell, "An assessment of website password practices," Computers & Security, 26(7-8), December 2007, pp. 445-451.

[5] Microsoft whitepaper, "Strong passwords: How to create and use them,"2006, Accessed Jan.31,2008,Availableat:http://www.microsoft.com/protect/yourself/password/create.mspx.

[6] [Online].Available:http://en.wikipedia.org/wiki/Phishing.

[7] Anti-Phishing Working Group. [Online]. Available:http://www.antiphishing.org.

[8] [Online].Available: http://en.wikipedia.org/wiki/Key${-}$logger.

[9] "One-time password-Wikipedia, the free encyclopedia,"[Online]: Available: https://en.m.wikipedia.org/wiki/One-time_password.[Accessed:Feb.12,2016].

[10] Rajan.S.Jamgekar, Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA", International Journal of Emerging Science and Engineering (IJESE), Vol-1, Issue-4, February 2013.

[11] Akanksha Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", International Journal on Computer Science and Engineering (IJSCE), Vol. 4 No. 09 sep 2012.

[12] Perrig.A, Szewczyk.R, Tygar.J.D, Wen.V and Culler D.E,"SPINS: Security Protocols for Sensor Networks",Wirel.Netw., vol. 6, no. 5, pp. 521-534, 2002.

[13] Widenbeck.S, Waters.J, Sobrado.L, and Birget.J, "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme", in Proc. Working Conf.Adv. Vis.Interfaces.