ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

An Investigative Analysis on Information Security

[1] Chandni B Menon [2] Anju Joy [3] Emilda Emmanuel [4] Dr. Vince Paul
[1][2][3] UG Scholars, [4] Professor and Head,
[1][2][3][4]Dept. of CSE Sahrdaya College of Engg and Tech, Kodakara, Thrissur, Kerala

***Abstract*— In this ultramodern but chaos world everything is at our fingertip. But this globalized village makes the human beings so crooked and selfish. Instead of fair and healthy competitions people started hacking our personal data. Hence the need of hour demands information security at its peak point ensuring Nano safety. Just like survival of the fittest theory human brains prevented the threat with lot of protection mechanisms like AES, DES, Blowfish, Rijndael, etc. This paper summarizes a clear study of these issues.**

Keywords:--Security, Bluetooth, Rijndael algorithm, AES, Blowfish algorithm, Protection, OTP, Authentication

I. INTRODUCTION

The present existing technology with picture password and numerical password for securing the files in a windows operating system are not widely accepted by the people. The survey proves that Key loggers, flash crowd, denial of services, proliferation of IOT, etc. affects security badly. The survey makes the fact clear that increasing the size of bits and licensed OS reduces the data insecurity. The e-learning and the e-world has made the dependence on computer like an inevitable factor like oxygen which demands highly confidential security measures.

II. LITERATURE SURVEY

Confidentiality has prime importance in the field of diplomatic and military matters. It uses the Bluetooth technology and OTP to personalize communication with the authorized party. MAC address stored in the computer registry. The previously used techniques were MEO File encryption XP, Safe House pro etc. In this MEO is a file encryption technique that encrypts file of any type. File encryption XP encrypts files using the blowfish algorithm. Safe House Pro provides confidentiality to our files. As the technology develops, and the data become portable the need of information security increases.

This system provides a decentralized security system with the help of unique MAC Address. It guarantees that the details won't be decrypted until the Bluetooth device is connected to the system and generated OTP during the process. So even if the inside or outsider attack can get the encrypted data, he cannot get the MAC Address and the keys which are stored in the Windows Registry. The keys used in the encryption process are generated internally inside the system. This guarantees the keys safety against the attack of the key logger and the algorithm generated OTP is send to the only user's device whose MAC address is currently used. The proposed system prevents any intruder attacks by encrypting the data with a Rijndael block cipher algorithm and prevents the unauthorized access. It keeps only the final cipher text and deletes the initial plain text and intermediate cipher texts that are generated during the encryption process [1]

To prevent unauthorized access, we provide a one-time password which changes on every login. After the Registration phase, the software on the computer system continuously scans for the registered Bluetooth device and if the registered device is found then the user is allowed to access all the features of the OS. If the registered device is found in the range in any phase, pseudo unique token is generated and is sent to the registered mobile device. Then it demands the user to enter the otp. If the entered token is matching it will ask for master password. If the entered master password is also valid then the operating system gets unlocked and its features are accessible to user. If the password doesn't matches, the user will have to wait for the next round of the Bluetooth scanning which will be repeating the same procedure all over again. [2] Bluetooth and the Rijndael algorithm used for Encryption and Decryption. This system has a client and server side. It functions with a computer and a mobile phone. The authorized phone from the client side and the system from the server side enables the application run smoothly. In AES, battery and time usage depends proportionally to the increasing key size without any data transfer. Attacks on DES proves that it has also got its own weaknesses. A primary host cannot determine whether that receiving host is on same link as it is bridged to that network segment.

Our proposed Rijndael algorithm requires two inputs. One is the key and other is the plain text and it performs number of rounds depending on size of the key such as 9,11,13 rounds are performed for the key size of 128,192,256 bits respectively. Each round consist of Adding a Sub key, Byte Substitution, Shift Row and Mixed Column. AES algorithm has a fixed key size whereas Rijndael algorithm has got variable key size. To obtain cipher text in Cipher Block Chaining mode, the initial vector is Xord with plaintext and thus obtained text is Xord with key. For further blocks the obtained cipher text undergoes the same process as before. Studies proves that the unique MAC address, and Bluetooth provides us with point to point security without any interference of an unauthorized person. [3]

To assure more security a Two Factor Authentication [T-FA] system is proposed using Bluetooth and Rijndael Encryption Algorithm. Coupling Bluetooth, which is used for short range communication and Rijndael algorithm which is an Advanced Encryption standard, believed to be the most effective technique for providing security. Users possessing administrator privileges has the complete right to create, modify and delete accounts as the password feature is interlinked with windows user accounts. Passwords helps in securing web-based and cloud based accounts. Passwords face several flaws corresponding to authorization, web and user interfaces and book marklet. Though biometrics and security tokens are some of the newly found alternatives to passwords, they increase the overall threat in information security and rise in infrastructural costs. [4]

The methods which provide password authentication are knowledge based, token based & biometric. Text password based and graphical password based technique comes under knowledge based authentication technique. Since the text based password can be easily attacked an alternative suggestion in this paper is to use graphical based password.The various examples for cued-recall click-based graphical password systems are pass point, cued-click points and persuasive cued click points. The guessing attacks, capture attacks and hotspot problems can reduce the security of pass points and cued-click points. Persuasive cued click points can overcome all these problems. This graphical based password is used for entering into the folder that is encrypted using Secure Hash algorithm.

In this methodology there are two steps. First is to create the graphical password(registration phase) and then login using the correct password. For password creation user will be provided with five click-points. As the first image is appeared; it has a small view port in it. Except the viewport all other areas are dimmed. Within the viewport the user has to select a click point. This click point can be selected anywhere in the picture by shuffling the viewport. The location or pixel value or tolerance area is stored in the database. Thus the five images are completed by five different click points. These images are stored in the database.

At the time of login if the pixel value of first image entered matches to the one entered at the password creation it will move to the next correct image. If the pixel value is wrong the next image generated will be wrong. Thus it is difficult for an intruder to attack into the system by selecting five correct pixel values. The pixel values are generated randomly and it is known only to the user. After successfully logged into system user can encrypt the desired folder using SHA algorithm. [5]

First the user required to register the MAC address of his Bluetooth enabled phone into the registry of windows. If the device is found in the range, validation is done by sending the MAC address to the system directly or by some android application. If the address match with the one stored in registry of windows user is allowed to access. User is also provided with the key to his mobile. Then the user can select the folders which he wants to decrypt among the encrypted files. If the registered mobile device is not in the range then all the files will get decrypted. [6]

In order to protect the files against unauthorized access, user encrypts it with a secret cryptographic key of symmetric cryptosystem. The popular standards for transferring keys are Bluetooth, IrDA and Wi-Fi. Among these Bluetooth is more secure.The plaintext is transformed and encrypted data is sent.These keys are saved within the authenticated parties. These random keys are generated using Random Key Generator (RNG) which is a computational device. The system asks for the plaintext and the first key. Then it checks whether the Bluetooth device is in range. After that the system generates one random key using RNG and encrypts the plain text to generate cipher text and it destroys the plaintext.

The system encrypts CT*1 using RK2 to generate second cipher text and destroys CT1. The final phase is encrypting CT*2 using RK3 to generate the final

CT*3 and destroys CT*2. Thus it will destroy all intermediate cipher text generated in the encryption process and holds only the final cipher text. These keys are encrypted using Rijndael algorithm before distributing via Bluetooth. In decryption process the cipher text needs to be transformed into plaintext. The system needs the MAC address of Bluetooth to match with the authenticated party. And then the decryption is done in reverse order of encryption. [7]

Asymmetric key cryptography is very much slower than symmetric key encryption. DES, AES, RSA, RC6 compared using various parameters such as computational time, memory usage, output bytes, Avalanche effect. The least encryption time is for DES algorithm and AES has least memory usage whereas RC6 requires longest encryption time and memory usage .Blowfish is more time consuming algorithm. RC6 requires less time for changing packet size.3DES is extension of DES,but it have low performance .Key size is large for 3DES, it will lead to time consumption and consumes more power.RSA is a block cipher asymmetric key encryption based on Number theory. Key generation, encryption, decryption are the operations performed in RSA algorithm. Two prime numbers p &q are used to generate keys. If p& q are small then the encryption is weak and p& q are large then more time consuming. DES is a block cipher, symmetric key encryption and size of key is 56 bits and size of block is 64bits.16 iterations are needed and it is insecure method. In 3DES 3 different keys are used and key size is 168 bits. First it will encrypt using k1, then decrypt using K2, finally encrypt with k3. AES supports any combination of data like 128, 192, 256 bits. For 128 bits10 rounds are needed, For 192 bits12 rounds, 256 bits14 rounds are needed.4 transformation is required: substitute bytes, shift rows, mix column transformation, add round key. In final step mix column transformation is avoided. [8]

DES, 3DES, AES, RC4 are compared on the basis of architecture, scalability, flexibility, security level. On the basis of architecture DES uses 64 bit block text and key size is 56 bits and performs 16 rounds.3DES is very slow but it is reliable since it uses longer keys.RC4 is stream cipher, data stream and generated key are XORed. Key length is 256 bit and performs 256 rounds. On the basis of scalability 3DES uses more memory space and performance is low. RC4 uses less memory space and hence provides high performance. On the basis of flexibility DES is not flexible, 3DES, AES, RC4 provides flexibility. On the basis of security level DES and RC4 does not provide high security because key size is 56 bits in DES.RC4 have poor key scheduling and fixed single key.3DES,AES provides high security.[9]

Single static password is not reliable as others can guess it. OTP is added for along with single static password.it is difficult for an intruder to login or abuse. Pseudo randomness or randomness algorithm is used to generate OTP, hence no one can find the OTP by observing previous OTP pattern. Time synchronized, mathematical algorithm are OTP generating algorithm. Each user gives token in Time synchronized algorithm.it is synchronized with clock. In mathematical algorithm new OTP are created by applying mathematical formula to previous OTP. To ensure the security encrypted OTP is send to user. [10]

For increasing the security three level authentication can include an integration of Text password, Graphical password and an OTPfor authenticating first the user needs to register his account using username, text password and email/mobile number. After the completion the next level of authentication is graphical based password. Pass points and Persuasive Cued Click Points are used in Graphical based password. It is a sequence of five different images with five different click points in it. At the time of registration the first image appears and user needs to select an appropriate click point for him. In such a way he completes four subsequent images. As the fifth image appears, this image will consists of four click points in it. Thus the registration is completed. At the time logging in into the system click points should be same as that of registration. If everything matches then the third level of three level authentication i.e. OTP is received through user's email or mobile text message. [11]

A graphical password is an authentication system that works with the images, presented in a graphical user interface (GUI).This kind of authentication mechanism involves alphanumeric passwords, images as security passwords, CAPTCHA and also a random number generator for security purposes. In the first level, the user is asked for finding a picture which the individual has already set during the password. If the selection is correct, then select certain numbers which has already chosen during account creation, from a set of rolling numbers. After that in second level of authentication, he may have to provide a textual password. Also, the user will be asked to enter the CAPTCHA correctly. Only three chances will be given for this final phase. If user went wrong, he can

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

try only after 5 hours. For this, timestamp can be utilized. This system actually enables click based and choice based techniques. The system can have a recognition based password or a recall based password depending on the application they choose. The application can use a set of faces for the same. [12]

The three levels for authentication can also be image ordering, color pixel selection and one time password. In image ordering user will be provided with a set of images. Among them he should select a set of images in same order. Next is the color pixel selection, in this user is provided with different blocks of colors. Then user can select a single color pixel among them. Next is the one time password generated to his registered mobile number which is valid only for a single session. Hash functions such as SHA-1 MD5 are used to generate OTP in the web part[13].

Two types of graphical password are recognition based graphical technique and recall based graphical technique. In recognition based graphical technique the user should memorize the images created at the time of registration. Pass faces, pass object are the two types of recognition graphical technique. In this the user should reproduce the image created at the time of registration. Like textual password it is difficult to remember. Two types of recall graphical technique are draw a secret and pass click. Madhuri Akhand, Ankitha Bijwe proposed single image pass click, multiple image pass click, pattern matching for folder security. In single image pass click select multi click points at the time of registration phase. At the time of login user should click the points. In second stage select images from a pool of images. If the two stages was successful a pattern should draw on a 2D grid using stylus or mouse and it should be continuous pen stroke. System uses five modules lock the folder, registration, login, reset password and server module. [14]

Collection of computers on internet is known as cloud. Data storage is one of the service provided by cloud. The data is stored somewhere in the server. The users can access, sync and back up the data. Dropbox, sugar sync, Amazon cloud Drive are providing storage .There are several cloud risk like shared access ,virtual exploits, authentication, authorization and access control, availability, ownership. Multiple, unrelated customers share the same CPU, storage, memory Known as multilenancy. It is a big issue because attacker can see all other data. Blow fish is a symmetric key encryption and it is fast, compact, simple and secure. Blowfish uses feistel structure. Blowfish algorithm have two steps key encryption and data encryption. Key expansion includes generating subkeys.521 iterations are required to generate all keys.16 iterations are needed for data encryption. Image based authentication along with OTP involved blowfish algorithm. At the time of login, user need to select images from a pool of images. If the first step was successful, then OTP will send to the registered mobile number or email". [15]

III. METHODOLOGY

The expanding dependence on computer systems has prompted the reliance on secret efforts to establish safety. Passwords has gotten to be a standout amongst the most universal cutting edge security instrument and is generally utilized for confirmation. What's more, this can be effortlessly remembered, thus expanding dangers. To beat the issues confronted by various security measures independently, we can utilize a mix of two or more security procedures. The prior figures can be broken easily on advanced calculation frameworks. In our review we arrived at a conclusion that expanding the span of bits and authorized OS decreases the information frailty. The greater part of the cryptographic calculations we have taken a gander at so far have some issue. Consequently we are wanting to build up a proficient algorithm for guaranteeing the security with expanded number of bits.

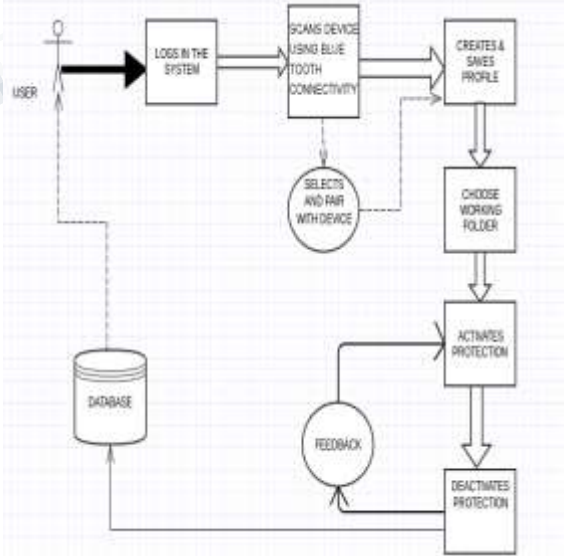

Fig.1 Block Diagram

One-Time passwords (OTP) have demonstrated their proficiency in securing different frameworks. So we propose a framework that makes utilization of OTPs to

give security to a framework. The proposed framework requires a Bluetooth empowered portable PC and a cell phone. A handshaking is done keeping in mind the end goal to distinguish the vicinity of cell phone. This handshaking procedure happens like clockwork. At the point when the gadget is not in the closeness, then the encryption is summoned. In the event that the gadget is recognized, then the framework prompts the client for password. At the same time, the OTP is sent to the client's registered cellular telephone. The client needs to make right sections for both the secret key and OTP furthermore the gadget should be kept close to the portable PC for the confirmation technique to work. This framework gives a three-variable verification to touchy information.

The framework is exceptionally easy to use and the interface keeps the client far from the foundation complexities. Therefore, this framework can be actualized to secure exceptionally private military data, or restorative information. The application discovers its utilization in science and examination fields, therapeutic field, and military field. In examination handle, this method can be utilized to encode information without loss of trustworthiness. This can likewise be utilized as a part of versatile social insurance systems to store data in cloud about ailment determination and points of interest. This gives higher measure of security to our envelopes.

IV. CONCLUSION

"Necessity is the mother of invention". All the existing cryptographic algorithms highlights the same security problems. These can be broken with ease on modern computation systems. So the need for an invention provided the use of a combination of two or more security processes.The invention and its application of a new and efficient algorithm with increased number of bitsprovides information security. The procedure is so simple. A Bluetooth laptop and mobile device are the only requirement for this. To detect the proximity of mobile device handshaking process is done in every five second. Encryption happens if the device is not in proximity. If in proximity the system seeks user for password and sends OTP to the registered mobile device. The correct entries of both the password and OTP provides decryption and the data visible. Thus the new system provides a three-factor authentication for sensitive data which in turn makes the entire procedure more secure.

REFERENCE

[1] Anurag Kurmi, Sushil Kumar Yadav, Amit Aher "Encryption and Decryption Application Based On Rijndael Algorithm and OTP Subsystem", International Journal of Scientific Research and Engineering Studies (IJSRES) Volume 1 Issue 5, November 2014.

[2] Aruna Gawde, Sanchit Jain, Mohsin Masani, Sahil Deliwalaa "Securing Computer Device Using Bluetooth technology and One-Time Password", International Journal of Engineering and Computer Science, Volume 4, April 2015.

[3] A.V.Nadargi, Apurva Dalmiya, Sonali Jadhav, Gajendra Singh Solanki "Study of Securing Computer Folders with Bluetooth", International Advanced Research Journal in Science, Engineering and TechnologyVol. 2, Issue 2, February 2015.

[4] Nikita Saple, Dhanraj Poojari, Ankita Kesarkar and Alka Srivastava, "Securing Computer Folders using Bluetooth and Rijndael Encryption" published at International Journal of Current Engineering and Technology, Vol.5, No.1. (Feb 2015)

[5] Ms. Shilpa. L. Dhapade, Prof. Nilmani Verma, "Implementation Of A Graphical Based Password For Folder Cryptography", International Journal of Engineering Research & Technology, Vol.2 - Issue 7. (July - 2013)

[5]Pharaoh Chaka, Hilton Chikwiriro, Clive Nyasondo (2014) "Improving The Windows Password PoliciesUsing Mobile Bluetooth And Rijndael Encryption", IJCSMC,Vol. 3, Issue.3.

[6] Apoorva Gulhane,Akant Preshin "Improving windows security with Rijndael encryption and Bluetooth" published at IJSTE vol2 issue09 march 2016.

[7] Wankhade S.B., Damani A.G., Desai S.J., Khanapure A.V.(2013), "An Innovative Approach to File Security Using Bluetooth" published at International Journal of Scientific Engineering and Technology Volume No.2, Issue No.5, pp : 417-423 1.

[8]Gurpreet Singh,Supriya "A study of encryption algorithm(RSA,DES,3DES,AES)for information security" published atInternational Journal of Computer Application vol:67,April 2013.

[9] Manju Rani, Dr.Sudesh Kumar"Analysis on different parameters of encryption algorithms for information security" published at International Journal of Advanced Research in Computer Science and software engineering vol:5,issue:8,Aug 2015.

[10] E.Kalaikavitha,Juliana Gnanaselvi "Secure login using encrypted Onetime password(OTP) and mobile based login methodology" published at Internatonal Journal of Engineering and Science vol:2,issue:10,Apr2013.

[11] Mr. Amit Kashinath Barate, Mrs.Sunita S. Shinde,Ms. Prajakta Umesh Mohite "Enhancement of Security Using Three Level Authentications ",International Journal of Engineering and Technical Research(IJETR)ISSN:2321-0869,Volume-2,Issue-8, August2014.

[12]Delphin Raj K M,Nancy Victor "A Novel Graphical Password Authentication Mechanism" International Journal of Advanced Research in Computer Science and Software Engineering 4(9), September - 2014, pp. 203-207 .

[13]Lalu Varghese, Nadiya Mathew, Sumy Saju, Vishnu K Prasad, "3-Level Password Authentication System" International Journal of Recent Development in Engineering and Technology (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014) 128.

[14] "Folder security using graphical password athentication scheme" by Madhuri Akhand,Ankitha Bijwe , Kajal zade, Karuna Borker international journal for Recent Research in mathematics computer science and information technology vol:2,issue:1,2015.

[15]. M Rama Raju, J Purna Prakash, "Protecting data in cloud storage using Blowfish encryption algorithm ad image based One-time password", Imperial journel of interdisciplinary Research vol:2, Issue:1,2016