An Approach For Improving Security of one Time Password Generation

Amit Verma[1], Nagendra Singh[2]
[1] Dept of CSE
[2] Assistant Professor Dept of CSE
[1, 2] Shri Ram Institute of Science & Technology, Jabalpur, Madhya Pradesh, India.

Abstract- *Internet services such as social networks, e-banking, email, cloud services, blogs, all require some form of security like user authentication. Despite the availability of advanced authentication technologies such as smart cards, biometrics or USB tokens, passwords and PINs are still the most prevalent form of user authentication. Graphical passwords are a form of user authentication on which a lot of research has been undertaken over the past decade and a variety of alternative password schemes proposed. Proposed system develops image based and portioning based authentication method. It provides user to select image and grid pattern for making partition password. It was found that brute-force attacks were largely ineffectual in terms of time required although image analysis had a profound impact on the effective password space. Password generated by this algorithm is more memorable than pass point mechanism. Proposed system is user friendly, effective, efficient, multifactor and multilayer authentication system. It keeps resistance against information leaks, brute force attack, phishing attacks, replay attack and man-in-the-middle attack.*

Keywords- Security, Authentication, Multifactor authentication, Graphical Password, Image Pattern, PAS.

I. INTRODUCTION

Physical security, network security and executive security are among those mechanisms that would secure organizations data. Each type has its own risks and implementations. The physical computer security is the type of security that is easiest to understand. Anyone who has physical access to the computer controls it such as—gadgets to secure the working space, locking sensors, human security, or constructing facilities [1]. That is, organizations resources must be physically secured because if an individual walk in, manipulates a computer and illegally access the network without prior authorization then information can be compromised. Worse is, compromised resources are prone to attacks and therefore proper physical security is important in preventing such attacks. Without durable physical security, an organization could spend thousands of dollars on anti-viruses, firewalls, and intrusion prevention systems only to have confidential data stolen by careless errors [2].

Authentication can be performed in many ways. The importance of selecting an appropriate authentication method is considered as the crucial decision in designing secure systems. It may be viewed as simply presenting credentials and authenticating the connecting party but failure to authenticate can compromise the network and the resources vulnerable to misuse [3]. To identify the user, a computer system or application will require authentication. Authentication is the process of establishing or making access to computer network, making purchases online, transferring accounts through bank website or perhaps visiting social media sites involve a method called authentication; [4][5] defined, authentication as the process of verifying the identity of a user, tracing the origins of an event, or ensuring that the information comes from a trusted site. It is the act of confirming the truth or genuineness of an attribute or entity. It establishes the authenticity or proves genuineness. The most common form of authentication is the use of username and password. Passwords are the most common form of authentication. To overcome the shortcomings associated with password authentication, the use of one time password was introduced to increase the level of security.

One-Time Password is a secure layer of security which enhances the security in terms of both authorization and authentication. OTP are passwords which are valid only once for an authentication. Its main advantage is that the user is free from impersonation and the password will not be reused. One-Time Password (OTP) is a generated string of characters and numbers that is used for authentication and valid only for a single transaction or session. OTP has been recognized in authentication technique for it increases the level of security and added features in protecting and securing confidential and sensitive information. OTP authenticates users by comparing two OTP values. One of them is generated by authentication server and the other is generated by clients. In the presented work we implement a strong OTP generation mechanism making use of multiple factors (TIH) that ensure user's Authentication [6].

Typically, an OTP is used in synchrony with static authentication information. When the user wants to log in, the system asks the user for his username, Password and in addition a One-Time Password. The username and password are static; they don't change for each and every attempt to log in and are therefore easy to remember. In contrast, the OTP will be different every time [7]. When the attacker tries to send a packet repeatedly, the system will notice that the One-Time Password is not accurate (it stays the same) and can issue a warning. In case the attacker manages to obstruct and send his packet first, then the user will notice something is wrong when his attempt to log in fails. One-time passwords are one way to resolve the vulnerability of static passwords to replay attacks to start the analysis and demonstration of the proposed endeavor.

OTP can be divided into three categories by the form of product such as OTP token, OTP card and mobile OTP [8]. There are some downside in OTP token and OTP card. First, the users can not be authenticated if they do not carry them. Second, if the users lose them, they should be reissued. Lastly, the users should have as many hardware’s as the number of services. Access controls exist to prevent unauthorized access. Companies should ensure that unauthorized access is not allowed and also authorized users cannot make unnecessary modifications. The controls exist in a variety of forms, from Identification Badges and passwords to access authentication protocols and security measures [9]. In this work we present a new solution for user authentication in an industrial scenario. In addition, we provide insights regarding the risks of the presented application and give indications for a secure implementation.

II. LITERATURE SURVEY

In 1981, Lamport [10] fIrst proposed a well known hash-based password authentication scheme. But the scheme suffers high hash overhead and password resetting problems. Then, Haller [11], [12] put forward the famous S /KEY OTP scheme. The basic thought of S / KEY OTP authentication is that: add some uncertain factors to the SPP (Secure Pass Phrase) of the users to carry out Hash calculation when login the systems so that the passwords, namely the OTPs are different from each other for each time. S / KEY OTP is the event-based OTP and it means that, both the client and server will typically have an identical initial seed (counter value). As the seeds on client and server may drift (due to passwords generated by client but not submitted, passwords submitted by client but does not reaches to server due to network failure, etc.), synchronizing the client's seed value stored at client and server is a major challenge in this method.

Since then, several schemes have been proposed to address this issue for achieving better functionality and efficiency. Raihi [13] proposed HOTP scheme and the HOTP algorithm is based on an increasing counter value and a static symmetric key known only to the token and the validation service. HOTP use the HMAC-SHA-l algorithm to generate one-time password. As the output of the HMAC-SHAI calculation is 160 bits, HOTP must truncate this value to something that can be easily entered by a user. Following that, in 2011 Raihi [14] proposed another

TOTP scheme which is based on time factor and the formula is: TOTP (K, T) = Truncate (HMAC-SHA- 1 (K, T)), where Time Factor T replaced counter value C. The main disadvantage of HOTP and TOTP scheme is that each HOTP generator has a different and unique secret K, which greatly increased the workload of key generation and management.
Due to the popularity of smart phone usages, the software-based OTP solutions bring no extra burden to the users and are economical to use. Hussein's scheme [15] generates OTP based on unique numbers in addition to the users behavioral biometric. The purpose of Hussein's system is to make the OTP more difficult, but his scheme is costly because it requires a special hardware; thus, this method cannot be applied in small- and medium-scale projects.

In 2015, Sun et al. [16] presented TrustOTP, a secure onetime password solution that can achieve both the flexibility of software tokens and the security of hardware tokens by using ARM TrustZone technology. However TrustOTP requires specific TrustZone hardware (such as Cortex-AS processor) and associated software, so it is not a feasible solution.

Philip T. Blythe et al [17] enhances the security in transport system by increasing the complexity in the circuitry inside the card so that fraudulent issues can be minimized. Here smart card with two interface and combi- cards is used. The drawback of this paper is that all the information is stored inside the card so that it can be easily hacked even though the circuitry is complex and the card can be used by anyone but in our paper all the information are stored only in the database and not in the card so that only the respective person can use the card.

Yahaya et al [18] presents combination on two security components which are the fingerprint recognition and smart card. The smart card plays a data storage for storing the cardholder's fingerprint data. The card holder is required to scan his/her fingerprint on the card for matching. Once it matches with the original finger print in the card then the money is deducted. The drawback is that as the card holds the original finger print when the card is stolen then it can be easily hacked and the copy of finger print can be easily matched. The second drawback is the finger print is scanned in the card itself so here the security is not up-to the level.

Fons M et al [19] includes two phases, the first phase is enrolment phase and the second phase is the authentication phase. In enrolment phase the user’s finger print is enrolled or stored in the data base or in the card and during authentication phase the users biometric is measured again. The main purpose of this work is to define the electronic architecture that permits to reach high performance at low cost and so they use on-chip technique and define a low cost platform with hardware-software design performance and dynamically reconfigurable hardware. The drawback in this paper is that image acquisition is a critical step, not only for enrolment stage but also for authentication phase. Subsequent recognition stage will only be effective if the acquired bitmap is a good quality image, so special attention must be taken during acquisition. If not, the system fails.

ByungRae Cha et al [20] explain that the OTP is an authentication method that is used to overcome the disadvantages of being exposed to tapping and attackers with bad intent. OTP is the first security medium for stability strengthening of electron financial transaction. The changes in the extracted characteristic point graphs due to change in location and angle can be used for creating different one time password keys from a single individual's fingerprint.

Aloul et al [21] describes that the Two-factor authentication system is found to be more secure than the one factor authentication system. The two factor authentication system needs token that has to be manufactured and distributed to the users. The mobile phones with GSM modem when used as a token are found to be a good alternate to other tokens and uses software securing. The two-factor authentication system using mobile phones as token is better than the one factor authentication system.

Edna et al [22] describes a two-factor authentication system that combines two independent credentials: what the user knows (PIN) and what the user has (Security token) to which the OTP is sent. It also proposes a secure payment solution involving four phases: Registration Phase, Login Phase, Ticket Requisition Phase and Ticket Generation Phase.

III. PROPOSED SYSTEM

To avoid any possible attacks in transaction like phishing, man-in-the middle attack, malware Trojans, the OTP must be secured. In order to provide a reliable and secure mode of transactions without any compromise to convenience, a reliable authentication scheme that combines the Image Based OTP with Advanced encryption (ECC) of the one-time password (OTP) has been developed in this paper. The Encrypted PIN can only be decrypted with well known keys. The key (OTP) is encrypted by using ECC. After the encrypted OTP SMS reaches the client’s mobile, or e-mail the PIN is used again for decrypting. The plain OTP text should be sent back to the server for verification to complete the transaction initiated. The proposed scheme provides security even if any disputes arise due any possible attacks like internet hacking, server hacking or mobile thefts.

New user should register in the system for utilizing it. At the time of registration availability will be checked and then user enter text details for fields like user name, text password, date of birth, address, city, phone number email id etc. System will show set of images, among them user should select any four images. These will be stored in the databases.

In authentication firstly text password based authentication will be performed. After that system will select one image from stored four images randomly and one text field of user randomly then generate OTP by encrypting selected text field with selected image. Encrypted OTP will be saved. OTP will be sent to users email id, which is used for OTP authentication. Proposed system uses SHA 512 image encryption for generating OTP, which will be more secure. At the time of authentication OTP entered will be decrypted to match with original one.

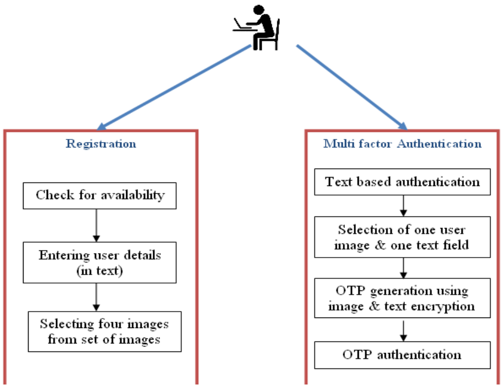

Registration
Check for availability
Entering user details (in text)
Selecting four images from set of images
Multi factor Authentication
Text based authentication
Selection of one user image & one text field
OTP generation using image & text encryption
OTP authentication

Figure 3.1: Working of proposed system

Main area of proposed work is to perform multifactor authentication based on strong OTP generation method. Proposed method is based on text encryption using image with SHA 512. Our proposed model contains three stages:

1. User Registration
2. OTP Generation
3. OTP Authentication

Following figure shows graphical representation of registration process

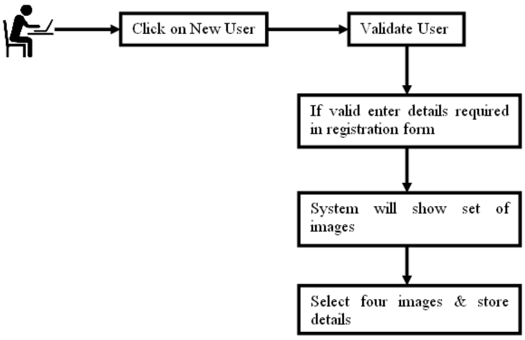

Click on New User
Validate User
If valid enter details required in registration form
System will show set of images
Select four images & store details

Figure 3.2: Registration process.

Proposed OTP generation method is based on text encryption of image based on SHA 512. The proposed system is based on a synchronous stream cipher that uses images, instead of passwords, as the secret key. A synchronous stream cipher is a type of symmetric key algorithm that generates a pseudo-random sequence of bits, called the key stream, independent of the plaintext and cipher text. These bits are then combined with the plaintext bits (usually using exclusive-or) to produce the cipher text, and then we select first eight character, which will be our OTP sent to users email id. Selection of images and text fields are random so it will produce more secure OTP. System will generate time based OTP.

Steps for OTP generation are as follows:-

Step-1. After successful text based login user session will be started and system will select one random image among set of four images and one random text field stored by the user at the time of registration.
Step-2. Load image & text field.
Step-3. Build the image vector for generating the key stream using hash function.
Step-4. Key stream bytes and text bytes are XOR.
Step-5. Convert output bytes to hexadecimal equivalent.
Step-6. Select first eight characters of cipher text which will be treated as OTP.
Step-7. Store OTP in session for OTP validation and start a timer for 1 minute. After 1 minute OTP will be expire.
Step-8. Send first eight characters of cipher text as OTP by email.

Steps for OTP Authentication are as follows:-
Step-1. User enters OTP received in email.
Step-2. System will check expiry time.
Step-3. If within time than it decrypt entered OTP & matched with stored encrypted OTP.
Step-4. If matched than user is authorized to do transaction, otherwise respond user with not matched message.

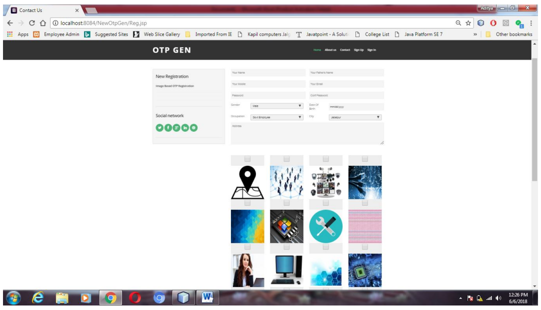
IV. IMPLEMENTATION AND EVALUATION

Following are minimum specifications for development of the system:

Table 1: Technical Specifications

Hardware Configuration	At least 1 GB free memory on storage disk, 512 MB RAM, Intel Pentium-4 Processor
Operating System	Windows 32-bit OS recommended
Software Configuration	Frontend – HTML Server side – JSP, Servlet Backend – MySQL
Development Tool	Netbeans IDE 8.0
Presentation Logic	HTML5, CSS

Figure below represents registration page with selection of four images randomly:


localhost:8084/NewOtpGen/Reg.jsp

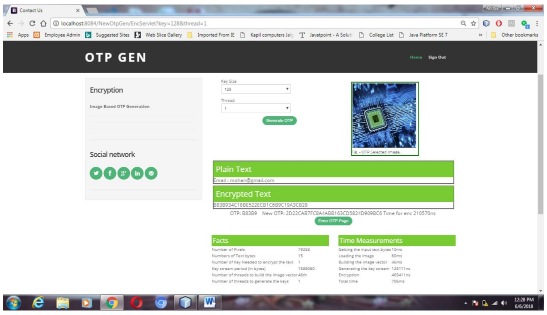
OTP GEN

New Registration
Image Based OTP Registration

Your Name | Your Father's Name | Your Mobile | Your Email | Password | Conf Password
Gender: Male | Date Of Birth: mm/dd/yyyy
Occupation: Govt Employee | City: Jabalpur
Address

Figure 4.1: Registration page

Figure below represents OTP generating page:


localhost:8084/NewOtpGen/EncServlet?key=128&thread=1

OTP GEN

Encryption
Image Based OTP Generation

Key Size: 128
Thread: 1

Fig. - OTP Selected Image.

Plain Text
Email : mohan@gmail.com

Encrypted Text
B83B934C18BE522ECB1C6B9C19A3CB28

OTP: B83B9 New OTP: 2D22CAB7FC8A4ABB163CD5824D909BC6 Time for enc 210570ns

Facts	
Number of Pixels	79253
Numbers of Text bytes	15
Number of Key Needed to encrypt the text	1
Key stream period (in bytes)	1585060
Number of threads to build the image vector	46th
Number of threads to generate the keys	1

Time Measurements	
Getting the input text bytes	10ms
Loading the image	60ms
Building the image vector	46ms
Generating the key stream	125111ns
Encryption	465411ns
Total time	706ms

Figure 4.2: OTP generation

Our proposed system surpasses all the problems of password based mechanism. It keeps resistance against the following security hazards and susceptibility:

Token Duplication: If an assaulter cannot steal the password he would try to duplicate it, hence it should not be written down. Along with it we have encrypted it with ECC algorithm.

Replay Attack: Since the OTP changes every time a user logs in. Replay attack would not be possible in this solution.

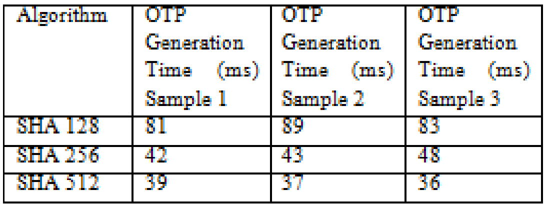
Eavesdropping: Storage of passwords in encrypted form makes eavesdropping almost impossible for attackers.

Man-in-the-middle attack: As the credentials are unrevealed to any third person and also the client and server use their public private keys for authentication, this attack is not possible.

For evaluating different algorithm we have taken three samples with fixed image and fixed text field. Experimental parameters are represented below in terms of table and chart for each sample.

Evaluation is on the basis of OTP Generation Time.

Table 2: Performance evaluation



Algorithm	OTP Generation Time (ms) Sample 1	OTP Generation Time (ms) Sample 2	OTP Generation Time (ms) Sample 3
SHA 128	81	89	83
SHA 256	42	43	48
SHA 512	39	37	36

All results shows that SHA 512 performs better in all samples for OTP generation as well as key stream generation.

V.CONCLUSION

Our proposed system Image Based OTP Generation surpasses all the problems of OTP based Authentication mechanism. It has been tested under various test cases with the results described in previous chapter. This authentication and generation solution is developed to petrify user access with reduced complications and increase user friendliness. Image Based OTP Generation keeps resistance against the following security hazards and susceptibility:

- Token theft.
- Token Duplication.
- Replay Attack.
- Eavesdropping.
- Man-in-the-middle attack.

REFERENCE

[1] Microsoft, Small and midsize businesses cloud trust study: U.S. study results, http://www.microsoft.com/enus/news/download/presskits/security/docs/ twcjune13us.pdf.

[2] R. Buyya, R. Ranjan, R.N. Calheiros, Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services, in: Algorithms and Architectures for Parallel Processing 6081/2010, in: LNCS, vol. 6081, 2010, p. 20.

[3] E. Carlini, M. Coppola, P. Dazzi, L. Ricci, G. Righetti, Cloud federations in contrail, in: Euro-Par 2011: Parallel Processing Workshops, in: Lecture Notes in Computer Science, vol. 7155, Springer, Berlin, Heidelberg, 2012, pp. 159–168.

[4] G. Anastasi, E. Carlini, M. Coppola, P. Dazzi, A. Lazouski, F. Martinelli, G. Mancini, P. Mori, Usage control in cloud federations, in: 2014 IEEE International Conference on Cloud Engineering (IC2E), 2014, pp. 141–146. http://dx.doi.org/10.1109/IC2E.2014.58.

[5] M. Coppola, P. Dazzi, A. Lazouski, F. Martinelli, P. Mori, J. Jensen, I. Johnson, P. Kershaw, The contrail approach to cloud federations, in: Proceedings of the International Symposium on Grids and Clouds (ISGC’12).

[6] Open Virtualization Format Specification, Version 1.1, Specification, DMTF (Jan. 2010).

[7] R. Buyya, R. Ranjan, and R. N. Calheiros, Inter Cloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services, Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2010), LNCS 6081, pp. 13-31, and 2010.

[8] Kremer, J., 2013. Virtualization and Cloud Computing, Steps in the Evolution from Virtualization to Private Cloud Infrastructure as a Service White paper on virtualization, USA.

[9] Rajesh, G., Sreenivasulu, G., 2014. The issues of cloud service delivery through virtualization of Dynamically Generated multiple virtual machine Services without missing deadline on the World Wide Web. Int. J. Curr. Eng. Tech. 4 (4), 2758–2762.

[10] "EC2 Instance Pricing – Amazon Web Services (AWS)." *Amazon Web Services, Inc.* N.p., n.d. Web. 27 Apr. 2017.

[11] D. Plummer, B. Lheureux, M. Cantara, T. Bova, “Cloud Services Brokerage Is Dominated by Three Primary Roles”, Gartner Research Note G00226509, 2011.

[12] Cloud Broker — A New Business Model Paradigm by Stefan Ried. Published: August 10, 2011, Updated: September 22, 2011.

[13] Cloud Brokers Will Reshape The Cloud - Getting Ready For The Future Cloud Business Models. Forrester, Sep. 2012.

[14] NIST, Cloud Computing Reference Architecture, National Institute of Standards and Technology, Special Publication 500-292, September 2011. Available on: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.

[15] N. Grozev and R. Buyya, "Inter-cloud Architectures and Application Brokering: Taxonomy and Survey," Software: Practice and Experience, vol. 44, no. 3, 2014, pp. 369–390.

[16] A. Ferrer et al., "Optimis: A Holistic Approach to Cloud Service Provisioning," Future Generation Computer Systems, vol. 28, no. 1, 2012, pp. 66–77.

[17] D. Petcu et al., "Experiences in Building a mOSAIC of Clouds," J. Cloud Computing, vol. 2, no. 1, 2013; doi: 10.1186/2192-113X-2-12.

[18] Y. Kessaci, N. Melab, and E.-G. Talbi, "A Pareto- Based Genetic Algorithm for Optimized Assignment of VM Requests on a Cloud Brokering Environment," Proc. IEEE Congress Evolutionary Computation (CEC), 2013, pp. 2496–2503.

[19] S. Nesmachnow, S. Iturriaga, and B. Dorronsoro, "Efficient Heuristics for Profit Optimization of Virtual Cloud Brokers," IEEE Computational Intelligence, vol. 10, no. 1, 2015, pp. 33–43.

[20] K.M. Sim, "Agent-Based Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 4, 2012, pp. 564–577.

[21] K.M. Sim, "Complex and Concurrent Negotiations for Multiple Interrelated E-Markets," IEEE Trans. Cybernetics, vol. 43, no. 1, 2013, pp. 230–245.

[22] A. Prasad and S. Rao, "A Mechanism Design Approach to Resource Procurement in Cloud Computing," IEEE Trans. Computers, vol. 63, no. 1, 2014, pp. 17–30.