International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 5, Issue 7, July 2018)

Security Enhancement & Risk Minimization Using Key Encryption

Vishakha Bharti[1], Amit Sinhal[2] Sanjay Mishra[3]
[1]M.Tech Scholar, Department of Information Technology, TIT Bhopal, vishakhabharti1993@gmail.com;
[2,] Head of Department, Department of Information Technology, TIT Bhopal, sinhal.amit@gmail.com, India;

Abstract – **Security has been an issue from the inception of computer systems. Secured systems must be usable to maintain proposed security. Password Authentication Systems have either been usable and insecure and not usable. Increasing either tends to complicate the other. Today, authentication is the principal method to guarantee information security and the most common and convenient method is password authentication. In this work proposed message digest5 (MD5) algorithm and cued click point algorithms for key encryption. In the proposed research work overcome the risks and provides maximum security.**

Keywords: **Authentication, Security, Key Encryption, Cued Click Point Algorithm, MD5, Cryptography, Steganography**.

I. INTRODUCTION

At present, computer networks constitute the core component of information technology infrastructures in areas such as power grids, financial data systems, and emergency communication systems. Protection of these networks from malicious intrusions is critical to the economy and security of our nation. Vulnerabilities are regularly discovered in software applications which are exploited to stage cyber attacks. Currently, management of security risk of an enterprise network is more an art than a science. System administrators operate by instinct and experience rather than relying on objective metrics to guide and justify decision making. In this report, develop models and metrics that can be used to objectively assess the security risk in an enterprise network, and techniques on how to use such metrics to guide decision making in cyber defense[1].

To improve the security of enterprise networks, it is necessary to measure the amount of security provided by different network configurations. The objective of our research was to develop a standard model for measuring security of computer networks. A standard model will enable us to answer questions such as “Are we more securing than yesterday?” or “How does the security of one network configuration compare with another?” Also, having a standard model to measure network security will bring together users, vendors, and researchers to evaluate methodologies and products for network security.

Good metrics should be measured consistently, inexpensive to collect, expressed numerically, have units of measure, and have specific context [2]. In this work meet this challenge by capturing vulnerability interdependencies and measuring security in the exact way that real attackers penetrate the network. In this work analyze all attack paths through a network, providing a metric of overall system risk. Through this metric, in this work analyze trade-offs between security costs and security benefits. Decision makers can therefore avoid over investing in security measures that do not pay off, or under investing and risk devastating consequences. Our metric is consistent, unambiguous, and provides context for understanding security risk of computer networks.

II. DATABASE SECURITY

Database security is essential because they suffer from security threats that may prove harmful and disastrous if disclosed or accessed publicly. Below it will present some security threats that are suffered by the databases.

Privilege Abuse: When database users are provided excessive privileges than their required functionality, then these privileges can be intentionally or unintentionally exploited.

Legitimate Privilege Abuse: In this attack, the attacker with the legitimate privilege access to the database may abuse the information stored in the database for the malicious purposes.

Privilege Promotion: The attacker in this attack takes advantage of the software vulnerabilities and errors and then elevates his clearance level to access the critical information stored in the database.

Operating System Vulnerabilities: In operating system vulnerabilities, the attacker exploits the vulnerabilities in the operating system to gain unauthorized access to the database for malicious reasons.

To alleviate these database security attacks many database security techniques have been proposed. Most of these techniques strengthen the access control mechanisms to restrict illegal access to the database.

In our paper discuss some of the common security techniques that can be used in addition to the access control mechanisms to store the data securely and in such a way that any outsider will not be able to understand the information, even if he is able to retrieve it[3].

III. RELATED WORK

Modelers generally think about security in terms of threats, risks, and losses [4]. Good models provide a rationale for measurements, and these models can be updated and calibrated as new data becomes available. A data model can also be used to automate security calculations. Some of the benefits of automating security metrics calculations are: Accuracy: Accuracy is required to trust the data that is collected and to develop consensus about the results. Repeatability: This is another important component of trust. If two measurements of a target can give the same consistent result, then the data can be trusted. Reliability: Automation of data collection will result in more reliability as it is not prone to human errors. Transparency: The steps used to derive the metrics are readily apparent, and they are accurately documented.

Security metrics have been suggested based on criteria compliance, intrusion detection, security policy, security incidents, and actuarial modeling. Statistical methods (Markov modeling, Bayesian networks, etc.) have been used in measuring network security. Complementary to our approach, measurements of attack resistance [5] and weakest successful adversary [6] have been proposed.

Early standardization efforts in the defense community evolved into the system security engineering capability maturity model (SSE-CMM) [7], although it does not assign quantitative measures. Lots of risk management work has been done at the National Institute of Standards and Technology (NIST) on risk identification, assessment and analysis. NIST Special Publication (SP) 800-55 [8] describes the security metrics implementation process. NIST SP 800-27 [9] describes the principles for establishing a security baseline. NIST SP 800-39 is the document that describes information security standards and guidelines developed by NIST.

The authentication password techniques used for security purpose .As authentication techniques generate passwords but they have to face attacks like dictionary attacks, brute force attacks, shoulder surfing. Authentication needs more powerful authentication techniques which remove all drawback of as mentioned above in authentication password techniques [10].

Now a day, graphical password is used as an alternative to text-based passwords, biometric and tokens. In this work use Graphical passwords because peoples can remember images better than the text. The Graphical passwords are divided into three categories: click-based graphical password, choice-based graphical password and draw-based graphical password [11].

IV. PROPOSED METHODOLOGY

Security in today's world is one of the important and challenging tasks that people are facing all over the world in every aspect of their lives. Databases are complex and many database security professionals do not have full understanding of risk and security issues related to different databases. To remove the security threats every organization must consists a security policy which should be implemented for sure.

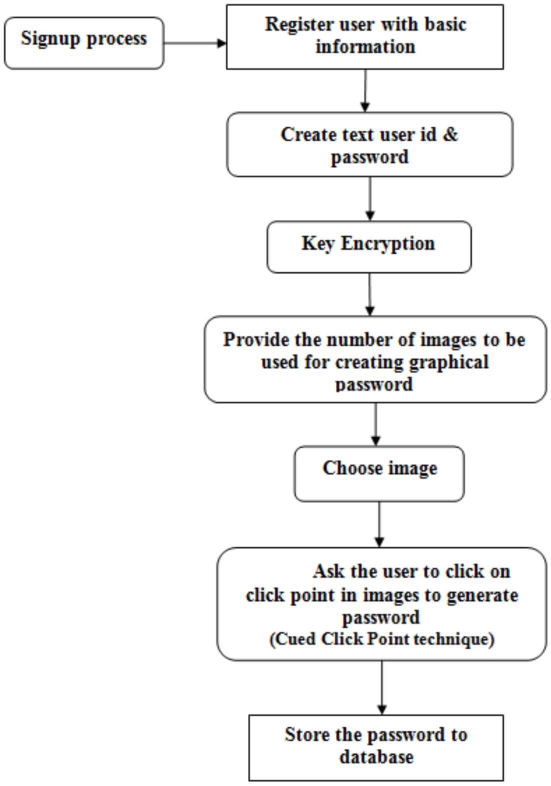

Signup process
Register user with basic information
Create text user id & password
Key Encryption
Provide the number of images to be used for creating graphical password
Choose image
Ask the user to click on click point in images to generate password (Cued Click Point technique)
Store the password to database

Fig.1 Flow diagram of User Registration Process

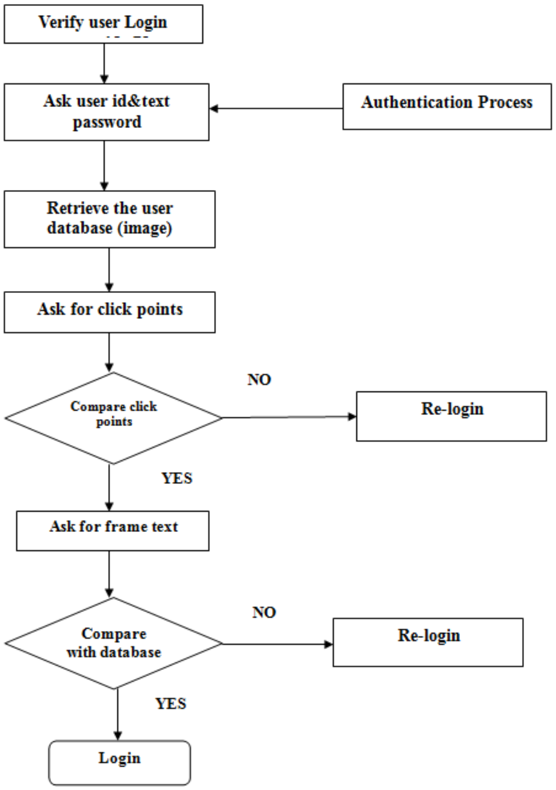


Fig.2 Flow diagram of Login Process

III.1. MD5 Algorithm

- Takes as input a message of arbitrary length and produces as output a 128 bit "fingerprint" or "message digest" of the input.
- It is conjectured that it is computationally infeasible to produce two messages having the same message digest.
- Intended where a large file must be "compressed" in a secure manner before being encrypted with a private key under a public-key cryptosystem such as PGP.
- Suppose a b-bit message as input, and that need to find its message digest.

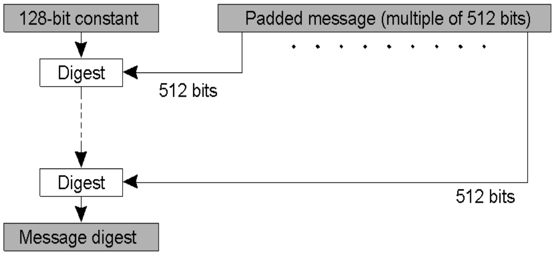


Fig.3 MD5 Algorithm Structure

III.2. Cued Click Point Technique

Cued Click Points (CCP) [12] is a proposed alternative to PassPoints. It can be viewed as a combination of PassPoints, Passfaces, and Story graphical method. A password consists of one click-point per image for a sequence of images. The next image has shown which is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in.

The prototype system did not hash the passwords or use a discretization method as would a actual system, but actually stored the particular pixel coordinates so that the users choice of click-points and their accuracy on re-entry could be examined. The system also implemented an improvised image selection process to reduce the size of the required image set since with several unique trials per participant, would have needed several thousand images to implement this technique. The first time a user clicked on a point, a new image was associated through that point. If a user clicked within the imaginary boundary of that point again, either to re-entering or to reset a password, the same image was shown.

Once related with a click-point, an image was not re-used for any other click-point during the entire session. Only areas where the user clicked on image will associate with them, so that reducing the total number of images required while still behaving in a consistent manner with the actual proposed scheme from the user's perspective. As already cleared in the implementation of passpoint, the images were 451x331 pixels in size and were displayed on a 19-inch screen with its resolution set to 1024x768 pixels.

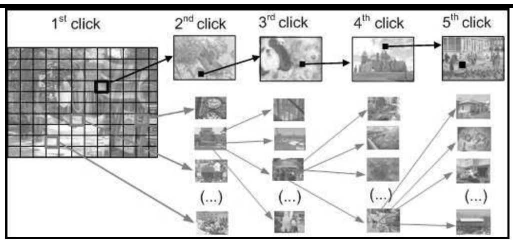


Fig.4 Cued Click Points method [10]

In Cued Click Point technique (CCP), users click one point on each of c = 5 images rather than on five points on single image. It proposed cued-recall and make known to visual signals that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the start). It also makes hotspot analysis more difficult to the attackers. As shown in Figure 4, each click results in showing a next-image, in effect leading users down a "path" as they click on their order of points. An incorrect click inclined to the erroneous path, with a clear indication of authentication failure only after the ultimate click. Users can select their image to the extent their click-point orders the next image. If they don't like resulting image, then they can create a new password concerning different click points to get different image.

Due to the complexity of today's connected critical infrastructure systems, their characteristics, variety of constraints, and their historical evolution, these systems might not, currently, implement a high-level of security assurances. The lack of a high level of security assurances may result from design, technical, implementation, or operational deficiencies, or a combination of these. These deficiencies can stem from a combination of inadequate [13].

V. RESULT DISCUSSION

Risk Management becomes a crucial part of every successful business model to deal with uncertain and risky socio-economic changes. Security concerns are a major player in minimizing risk in businesses by protecting its intangible resources and knowledge. The proposed research work is implemented in MATLAB tool using different algorithm and their results shown in below:

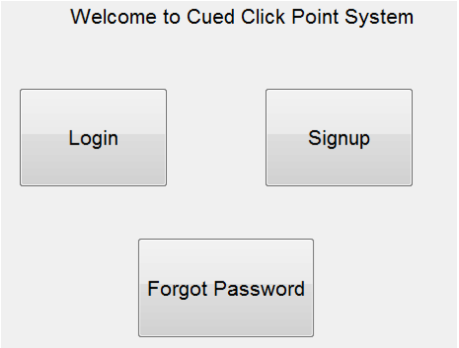
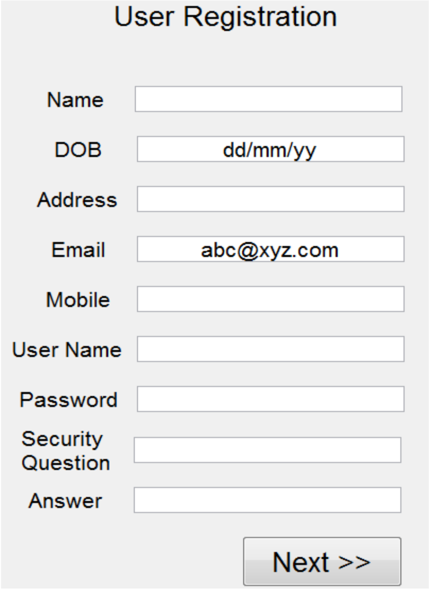


Fig.5 Overall Proposed System in GUI window

Figure 5 shows the overall system of proposed research. In this system three mainly functions are implemented. Signup for new user registration, login for registered user and forgot password for when forget your registered password.


User Registration

Name

DOB dd/mm/yy

Address

Email abc@xyz.com

Mobile

User Name

Password

Security Question

Answer

Fig.6 Sign up Function

Figure 6 Sign up function. In this function new user register. For user registration enter the name, DOB, Address, Email, mobile, user name, password, security question, and their answer. In this function key encryption algorithms are used. The MD5 algorithm is used for this function.

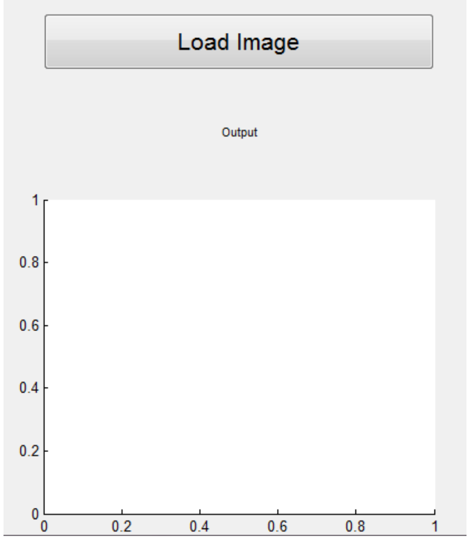
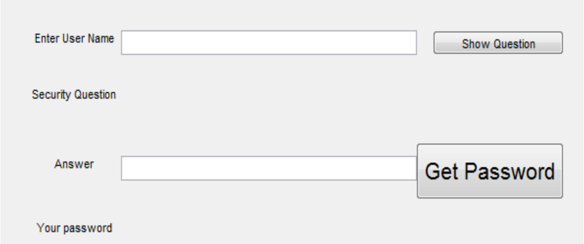


Fig.7 Login Page

Figure 7 shows login function. In this function registered users are login for the next step. This function implemented by using cued click point algorithm. It can be viewed as a combination of PassPoints, Passfaces, and Story graphical method. A password consists of one click-point per image for a sequence of images.


Enter User Name

Security Question

Answer

Your password

Fig.8 Forgot password

Figure 8 shows forgot password function. In this function enter user name and security question and shows answer and lastly get password.

Table 1 Comparison of previous and proposed work

Work	Algorithm	Login Feature	Authentication Process	Security Level
Previous	Account Control Policies, Audit Control Policies, Windows Firewall, SecurityControl Options	Yes	No	1
Proposed	MD5, Hash Function, Cued Click Point	Yes	Yes	2

VI. CONCLUSION

This methodology can be applied to evaluate and improve the security risk of enterprise systems. In the proposed research presented different algorithm for different function. In this work proposed key encryption MD5 algorithm for signup function and cued click point techniques are used for login function. The proposed method has advantages over PassPoints, Cued Click Point, and Persuasive Cued Click Point in terms of usability and also security. Being click point as on images shown and having to remember click-point on given image appears easier than having to remember an ordered series of clicks. In this also proposed hesh function. All the proposed algorithm work overcome the risks and improves the security.

REFERENCES

[1] Kumar, Basant, and Mahmood Hamed Said Al Hasani. "Database security—Risks and control methods." Computer Communication and the Internet (ICCCI), 2016 IEEE International Conference on. IEEE, 2016.

[2] Malik, Mubina, and Trisha Patel. "Database security-attacks and control methods." International Journal of Information Sciences and Techniques (IJIST) 6.1/2 (2016).

[3] Shameli-Sendi, Alireza, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. "Taxonomy of information security risk assessment (ISRA)." Computers & security 57 (2016): 14-30.

[4] Kalaiprasath, R., R. Elankavi, and Dr R. Udayakumar. "Cloud. Security and Compliance-A Semantic Approach in End to End Security." International Journal Of Mechanical Engineering And Technology (Ijmet) 8.5 (2017).

[5] Chen, Min, et al. "Software-defined mobile networks security." Mobile Networks and Applications 21.5 (2016): 729-743.

[6] Sajid, Anam, Haider Abbas, and Kashif Saleem. "Cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges." IEEE Access 4 (2016): 1375-1384.

[7] Singhal, Anoop, and Xinming Ou. "Security risk analysis of enterprise networks using probabilistic attack graphs." Network Security Metrics. Springer, Cham, 2017. 53-73.

[8] Kayarkar, Harshavardhan. "Classification of various security techniques in databases and their comparative analysis." arXiv preprint arXiv:1206.4124 (2012).

[9] Yih-Chuan Lin, Tzung-Shian Li, Yao-Tang Chang, Chuen-Ching Wang, Wen-Tzu Chen, “A Subsampling and Interpolation Technique for Reversible Histogram Shift Data Hiding”, Image and Signal Processing, Lecture Notes in Computer Science, vol. 6134, 2010, Publisher: Springer Berlin/Heidelberg, pp. 384-393.

[10] Priti Jadhao, Lalit Dole- Survey on Authentication Password Techniques, (IJSCE) International Journal of Soft Computing and Engineering, Volume-3, Issue-2, pp.67-68,May 2013.

[11] P. R. Devale Shrikala M. Deshmukh, Anil B. Pawar- Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme , (IJSCE) International Journal of Soft Computing and Engineering , Volume-3, Issue-2, pp.280-283,May 2013.

[12] Chyuan-Huei Thomas Yang, Chun-Hao Hsu, “A High Quality Reversible Data Hiding Method Using Interpolation Technique," IEEE Fifth International Conference on Information Assurance and Security, vol. 2, 18-20 Aug. 2009, pp. 603- 606.

[13] Ananth A. Jillepalli et al. “Security Management of Cyber Physical Control Systems Using NIST SP 800-82r2”, 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, 2017, pp. 1864-1870.