QUANTUM CRYPTOGRAPHY BASED GRAPHICAL AUTHENTICATION SYSTEM

Makasare Jacob Joseph, Kadu Ajinkya Jaysing, Bhalerao Aniruddha Girish,

Kadu Jaideep Sunil, Shirsath Somnath Sopan.

Ms. Kalyani T. Bhandwalkar - Assistant professor

Pravara Rural Engineering College, Loni

Abstract:-

Credentials consisting of customer identifiers, passwords, and keys may be stolen by an attacker when they are poorly managed. As an example, a poorly controlled personal pc (computer) inflamed with malicious software (malware) is a smooth goal for credential attackers. On the other hand, channel-breaking attacks that permit eavesdropping on the conversation between customers and a monetary institution are another form of exploitation. In a phishing system, think cheater sends out heaps of phishing emails with a hyperlink to the fake internet site. Victims click on hyperlinks in email believing it is legitimate. They input non-public information on the fake internet site. Fraudsters collect the stolen records and login into the correct internet site. This is an overall technique of phishing. Manually the password can be obtained by the user while the user is typing it into the system field. To overcome all the above issues following article provide a secure cryptography-based system. Though the system is time-consuming and less efficient for human memory. But it provides a secured option to the system.

Keywords:-Quantum Cryptography, Image Processing, Classification, Shoulder Surfing, Training Images, OTP, Secret Bit Key logging etc.

Introduction:-

Threats in opposition to electronic and financial offerings may be classified into two foremost instructions: credential stealing and channel breaking assaults. Credentials consisting of customer's identifiers, passwords, and keys may be stolen by an attacker when they're poorly managed. As an example, a poorly controlled personal computer inflamed with malicious software (malware) is a smooth goal for credential attackers. On the other hand, channel-breaking attacks that permit eavesdropping on the conversation between customers and a monetary institution are another form of exploitation. At the same time as the classical channel, breaking assaults can be avoided through the proper utilization of a protection channel inclusive of IPSec and at ease sockets layer (SSL), recent

channel breaking attacks are extra challenging. Indeed, key logging assaults or people who make use of session hijacking, phishing, and pharming, and visible fraudulence cannot be addressed by using simply enabling Quantum Cryptography. The shoulder browsing attack is an assault that can be achieved with the aid of the adversary to accumulate the individual's password by searching over the user's shoulder as he enters his password. However, most of the current graphical password schemes are liable to shoulder-browsing a recounted hazard wherein an attacker can seize a password through a direct statement or by recording the authentication consultation. Because of the visual interface, shoulder-

browsing becomes an exacerbated problem in graphical passwords. A graphical password is easy than a textual content-based password for the majority to undergo in thoughts. Suppose an eight-man or woman password is critical to benefit access into a specific computer network. Sturdy passwords may be produced which might be proof against guessing, dictionary assault. Key-loggers, shoulder-surfing, and social engineering.

Literature Survey:-

Graphical password is one of the alternative solutions to the alphanumeric password as it is a very tedious process to remember an alphanumeric password.[1]

Improving the security of the systems relies on recognition-based, rather than recall-based authentication.[2]

Graphical password using passpoints and three longitudinal trials for six weeks.[3]

A usability comparison between a new mechanism for user authentication –Passfaces and passwords.[4]

Security designers must identify the causes of undesirable user behavior, and address these to design effective security systems.[5]

Framework provides an evaluation methodology and benchmark for future web authentication proposals.[6]

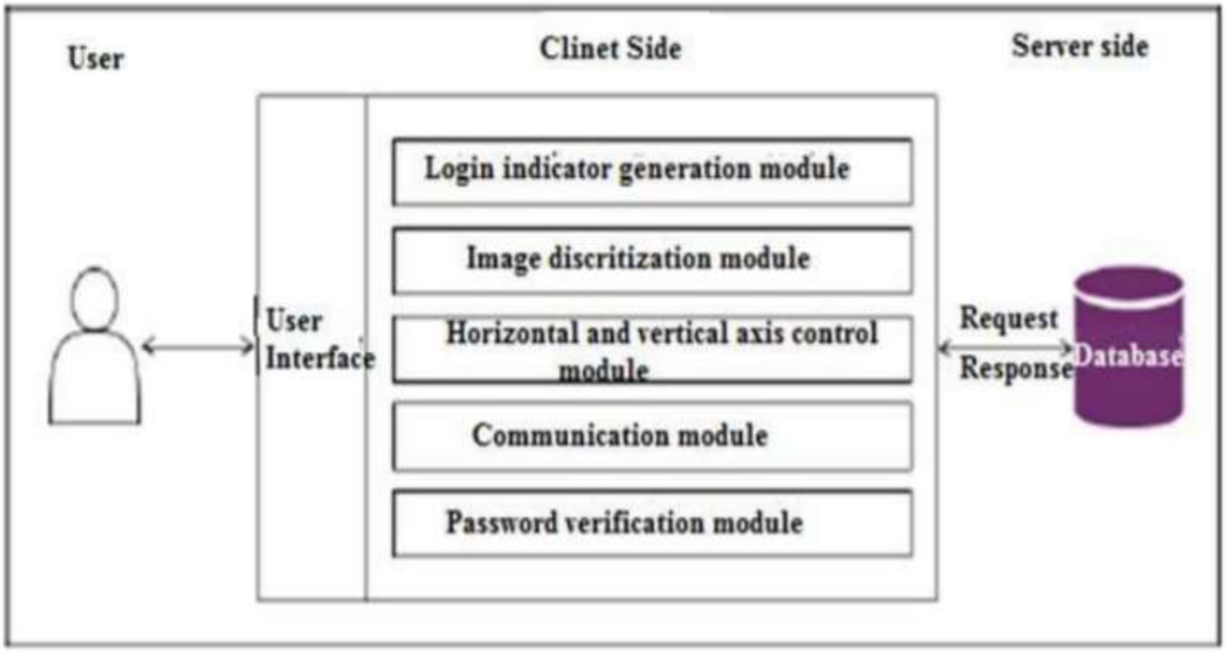
To establish a secure basis for online communication, we propose SafeSlinger, a system leveraging the proliferation of smartphones to enable people to securely and privately exchange their public keys. Through the exchanged authentic public keys, Safe- Slinger establishes a secure channel offering secrecy and authenticity, which we use to support secure messaging and file exchange.[7]

To propose Mobile Password Authentication (MP-Auth) to counter such attacks, which cryptographically separates a users long-term secret input from the client PC, and offers transaction integrity.[8]

To propose a user authentication scheme named Cover- Pad for password entry on touchscreen mobile devices. CoverPad improves leakage resilience by safely delivering hidden messages, which break the correlation between the underlying password and the interaction information observable to an adversary.[9]

To present GAnGS, a fully-implemented system for exchanging authentic information between mobile de- vices when they are physically present in the same location. GAnGS is scalable, appropriate for two or more devices. We implement two user friendly variants of GAnGS on Nokia N70 camera phones. The first vari- ant, GAnGSP, is based on an untrusted communication hub. The second variant, GAnGS-T, needs no infrastructure. Both variants use Bluetooth for peer-to-peer wire- less communication during the information exchange.[10]

System Architecture:-


User
Clinet Side
Server side
Login indicator generation module
Image discritization module
Horizontal and vertical axis control module
Communication module
Password verification module
User Interface
Request
Response
Database

It includes client's side as well as server side Database. User works on following items of client's side 1.Login indicator generation module.

2.Image discritization module.

3.Horizontal and vertical axis control module.

4.Communication module.

5.Password verification module.

At the server side the data is to be stored in the database.

It includes three phases

1.Registration Phase.

The Username, password and other credentials are inputted to the fields.

2.Authentication phase.

The entered data in Registration phase is authenticate with database data which is on sever on server side.

3.Output.

Secure and authenticated system based on Quantum Cryptography.

Dataflow Diagaram:-

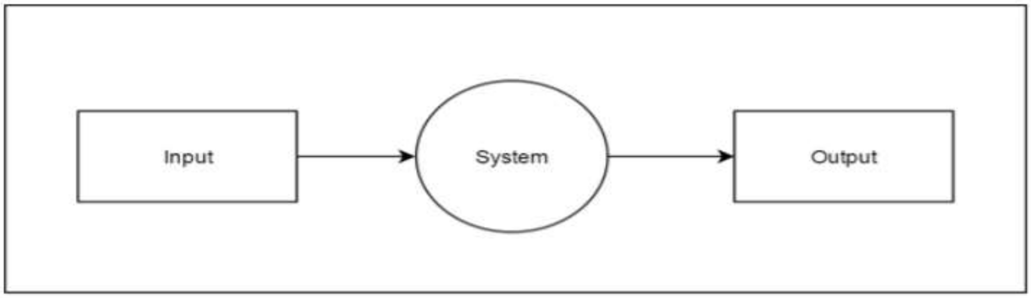


Figure 4.2: DFD Level 0

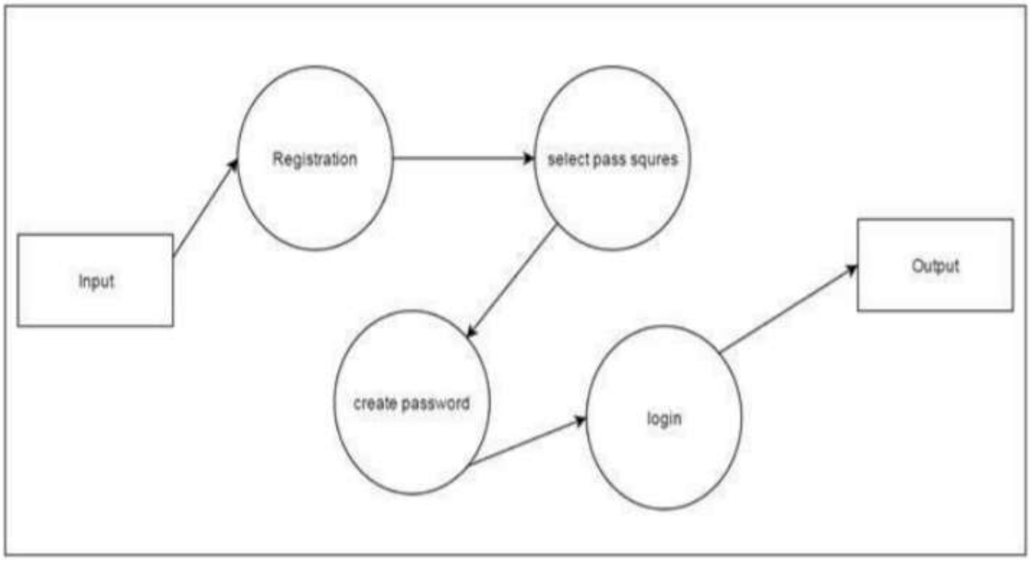


Figure 4.3: DFD Level 1

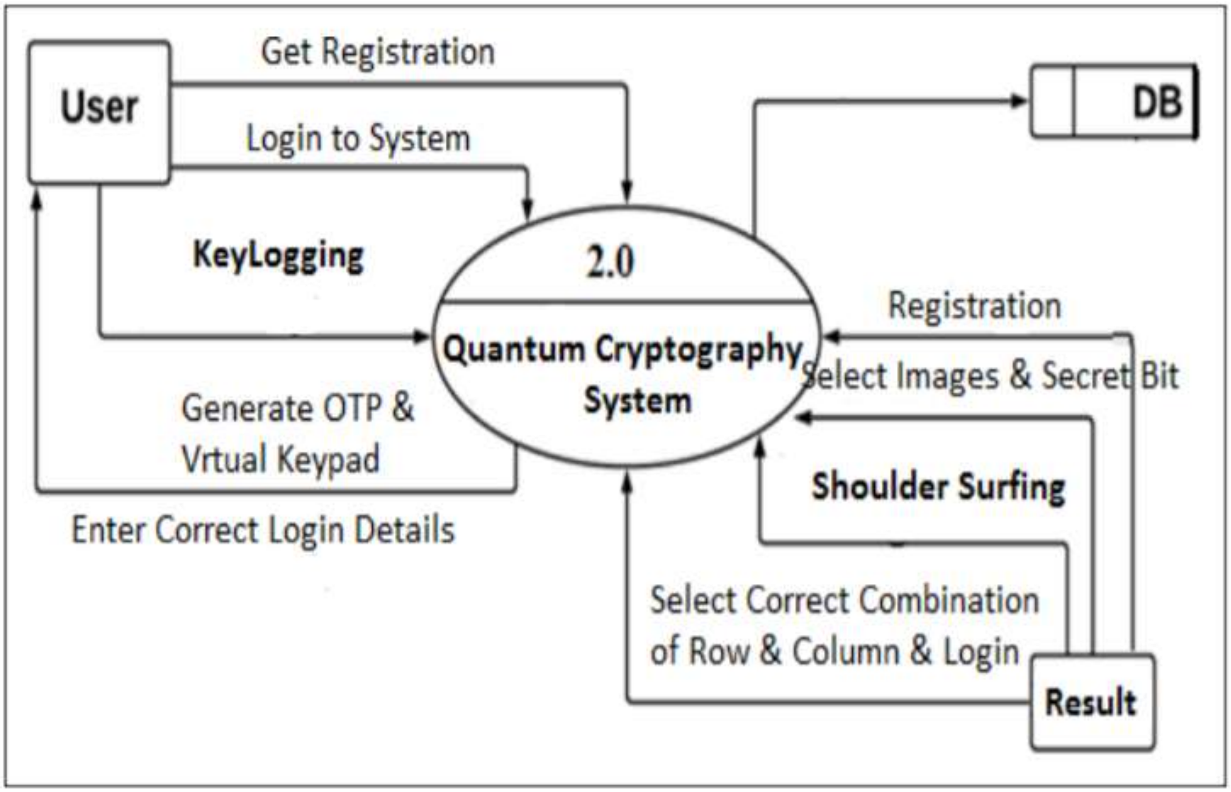

User
Get Registration
Login to System
DB
KeyLogging
2.0
Quantum Cryptography System
Registration
Select Images & Secret Bit
Generate OTP & Vrtual Keypad
Shoulder Surfing
Enter Correct Login Details
Select Correct Combination of Row & Column & Login
Result

Figure 4.4: DFD Level 2

Applications:-

1. ATM Transactions
2. Card Security
3. Electronic Transaction Processing (ONLINE BANKING)
4. UPI Transactions Apps
5. Securing Online Documents with Sensitive information

Conclusion:-

1.We proposed a system that uses user-driven visualization to improve protection and prevent the system from shoulder Surfing.

2. In this paper, we proposed a way for online account authentication and Fraud Transaction prevention in addition to offering protection for confidential information through the usage of extended visual cryptography and its strategies.

3. Preventing phishing attacks by using a graphical password encryption algorithm.

References:-

1. Gurav, Shraddha & Gawade, Leena & Rane, Prathamey & Khochare, Nilesh. (2014). Graphical Password Authentication: Cloud Securing Scheme. 479-483. 10.1109/ICESC.2014.90.

2. Rachna Dhamija Adrian Perrig. “Deja Vu: A User Study Using Images for Authentication”. 2000. Proceedings of the 9th conference on USENIX Security Symposium - Volume 9. USENIX Association, USA.

3. Susan Wiedenbecka, Jim Watersa, Jean-Camille Birgetb, Alex Brodskiyc, Nasir Memon. "PassPoints: Design and longitudinal evaluation of a graphical password system". International Journal of Human Computer Studies, 63*(1-2), 102-127.* https://doi.org/10.1016/j.ijhcs.2005.04.010

4.Brostoff S., Sasse M.A. (2000) Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In: McDonald S., Waern Y., Cockton G. (eds) People and Computers XIV — Usability or Else!. Springer, London. https://doi.org/10.1007/978-1-4471-0515-2_27

5. Martina Angela Sasse, Sacha Brostoff Dirk Weirich. "Transforming the Weakest Link: A Human-Computer Interaction Approach for Usable and Effective Security".

6. Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajanoy. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes (2012)". International Journal of Scientific & Engineering Research, Volume 4, Issue 4, April-2013 704

7. M Farb, Yue-Hsun Lin, Tiffany Hyun-Jin Kim, Jonathan McCune, A Perrig. "SafeSlinger: Easy-to-Use and Secure Public-Key Exchange (2011)".

8. Mohammad Mannan and P.C. van Oorschot. "Leveraging Personal Devices for Stronger Password Authentication (2011)". International Journal of Innovative Research in Science, Engineering and Technology

9. Qiang Yany, Jin Hanz, Yingjiu Liy, Jianying Zhouz, Robert H. Dengy. "Designing Leakage-Resilient Password Entry on Touchscreen Mobile Devices (2013)".

10. Chia-Hsin Chen, Chung-Wei Chen, Cynthia Kuo, Yan-Hao Lai, Jonathan M. McCune, Ahren Studer, Adrian Perrig, Bo-Yin Yang, Tzong-Chen Wu. "GAnGS: Gather, authenticate n Group Securely (2008)". In Proceedings of the ACM Annual International Conference on Mobile Computing and Networking (MobiCom