Scientific Journal of Impact Factor (SJIF): 4.14
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 12, December -2016

Retrieval Of information Using QR code

[1]Preshit Sheth, [2]Mayur Charde, [3]Rishikesh ligaade, [4]Prof. Snehal Kanade

[1,2,3,4]Dept Of Info.Tech,SKN,Lonawla,Pune

Abstract---*Keylogging or keyboard capturing is that the activity of recording (or logging) the keys affected on a keyboard, usually in an exceedingly tightlipped means in order that the individual utilizing the keyboard is unconscious that their activities area unit being ascertained. It likewise has exceptionally authentic uses in investigations of human-computer interaction. There are a unit varied Keylogging techniques, extending from hardware and code based mostly methodologies to acoustic examination. Together with human in authentication protocols, whereas guaranteeing, isn't straightforward in light-weight of their restricted capability of calculation and remembrance. We tend to exhibit however careful mental image define will improve the safety yet because the convenience of authentication. We tend to propose 2 visual authentication protocols: one may be a one-time-password protocol, and also the alternative may be a password-based authentication protocol. Our approach for real arrangement: we tend to have the capability attain to associate abnormal state of easy use whereas fulfilling demanding security requirements.*

Keywords---*Keylogging, One-Time-Password Protocol, Password-Based Authentication Protocol, QR Code.*

I. INTRODUCTION

Nowadays, attributable to increase in variety of road accidents there's a requirement to access a person's medical/contact data just in case of emergencies for aid and hospital & different formalities. so as to shorten the admitting procedures once a patient seen within the emergency department is after admitted to the hospital, we are going to be retrieving their data hold on in cloud information that is scanned with the assistance of a QR Code containing a link to the victim's emergency data. This may facilitate hospital authority to grant acceptable medication to the accident victim and inform his/her family.

In order to shorten the admitting procedures once a patient seen within the emergency department is after admitted to the hospital, we are going to be retrieving their data that is scanned with the assistance of a QR Code containing a link of the victim's emergency data hold on in cloud information. Initially, the user has to feed his data into the information. Then, we are going to generate a 2nd dynamic QR Code with the assistance of a singular uniform resource locator. This 2nd dynamic QR Code is provided to the users within the sort of a sensible card.

This data may be accessed by the user to either read or modify it via organizations web site. For accidental emergency functions this data are accessed by the approved users (police and/or the medical authorities) via a company specific login. If login is fortunate, the QR Code of the victim that contains his/her emergency data may be scanned. After scanning of QR Code, a link is retrieved. On clicking this link, the victim's details are retrieved from the most information.

II. PROPOSED SYSTEM

Two protocols for authentication countersign-based authentication and one-time password based mostly authentication that uses mental image by technique for exaggerated reality to relinquish each high security and high convenience. Each conventions supply nice circumstances in lightweight of mental image each as so much as security and convenience. Model utilization as humanoid applications that demonstrate the convenience of our conventions in true organization settings.

III. SYSTEM ARCHITECURE

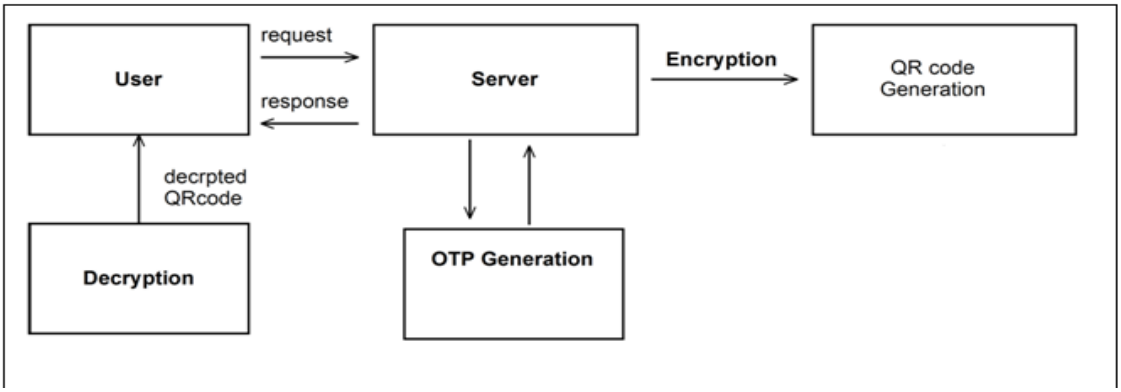

Figure 1. Architecture Diagram of Proposed System

IV. MATHEMATICAL MODEL

Let W be the whole system which consists

Input = {U, M, C, k, S, Pvk, Pbk, M}.

1. Let u is the set of number of users.

   U= {u1, u2,…..un}.
2. k is the secret key used for encryption.
3. M is the message sent from the set M.
4. C is the cipher-text in the set C
5. S is the signature generated for sending message.
6. Pvk is the private key.
7. Pbk is the public key.

Functions:

1. Encrk (): an encryption algorithm which takes a key k and a message M from set M and outputs a cipher-text C in the set C.
2. Decrk (·): a decryption algorithm which takes a ciphertext C in C and a key k, and outputs a plain-text (or message) M in the set M.

3. Sign (·): a signature generation algorithm which takes a private key Pvk and a message M from the set M, and outputs a signature σ.
4. Verf (·): a signature verification algorithm which takes a public key Pbk and a signed message (M, σ), and returns valid or invalid.
5. QREnc (·): a QR encoding algorithm which takes a string S in S and outputs a QR code.
6. QRDec (·): a QR decoding algorithm which takes a QR code and returns a string S in S.

Procedure:

A. Protocol for generating OTP for Authentication with Random Strings

Step1: The user connects to the server and sends her ID.

Step2: The server checks the ID to retrieve the user's public key Pbk from the database. The server then picks a fresh random string OT P and encrypts it with the public key to obtain
EOT P = EncrPbk (OT P).

Step3: A QR code QREOT P is displayed prompting the user to type in the string.

Step4: The user decodes the QR code with EOT P = QRDec (QREOT P). Because the random string is encrypted with user's public key (Pbk), the user can read the OTP string only through her smart phone by OT P = Decrk (EOT P) and type in the OT P in the terminal with a physical keyboard.

Step5: The server checks the result and if it matches what the server has sent earlier, the user is authenticated. Otherwise, the user is denied. In this protocol, OT P is any combination of alphabets or numbers whose length is 4 or more depending on the security level required.

B. Protocol for Authentication with Password and Randomized Onscreen Keyboard

Step1: The user connects to the server and sends her ID.
Step2: The server checks the received ID to retrieve the user's public key (Pbk) from the database. The server prepares π, a random permutation of a keyboard arrangement, and encrypts it with the public key to obtain EKBD = EncrPKID (π).

Step3: Then, it encodes the cipher-text with QR encoder to obtain QREKBD = QREnc (EkID (π)). The server sends the result with a blank keyboard.

Step4: On the user's terminal, a QR code (QREKBD) is displayed together with a blank keyboard. Because the onscreen keyboard does not have any alphabet on it, the user cannot input her password.

Step5: The user executes her smart phone application which first decodes the QR code by applying QRDec (QREKBD) to get the cipher text (EKBD). The cipher text is then decrypted by the smart phone application with the private key of the user to display the result (π = DecrSKID (EKBD)) on the smart phone's screen.

Step6: When the user sees the blank keyboard with the QR code through an application on the smart phone that has a private key, alphanumeric appear on the blank keyboard and the user can click the proper button for the password. The user types in her password on the terminal's screen while seeing the keyboard layout through the smart phone. The terminal does not know what the password is but only knows which buttons are clicked. Identities of the buttons clicked by the user are sent to the server by the terminal.

Step7: The server checks whether the password is correct or not by confirming if the correct buttons have been clicked. Some of the technical issues in the two protocols that we have introduced in the previous sections call for further discussion and clarification. In this section, we elaborate on how to handle several issues related to our protocols, such as session hijacking, transaction verification, and securing transactions.

V. METHODOLOGY USED IN SYSTEM

5.1 Registration Process

In this stage, the user can fill an internet kind provided by the organization on their web site. This on-line kind is going to be consisting of all needed details for the info. Information hold on in info and presented user. When with success filling the net kind, the data are going to be hold on within the info and therefore the webpage which can contain all the small print of the user are going to be shown to the user. The info is going to be hold on within the cloud.

5.2 Generate QR Code

After made registration of user the QR code is generated by the system. Using the distinctive computer address generated for the webpage of every user, distinctive second QR codes are going to be generated for every user.

5.3 Causing confirmation mail containing the QR code to the user

A confirmation mail containing the distinctive second QR code and secrete key that is employed to decode that QR code of the user are going to be sent to the user when the QR code is generated with success.

5.4 Scan QR code

A smart phone application are going to be used for scanning the QR code. before scanning the QR code, approved login are going to be provided to the actual authorities like police, hospital management, or admin and therefore the user itself.

5.5 Link retrieval and show link

After scanning the QR code, links are going to be retrieved and exhibited to the user scanning the QR code.

5.6 Show data of the victim/user.

After displaying the link, the user ought to click on the link then the webpage or a page consisting of that user's details are going to be displayed.

VI. CONCLUSION

We planned and analyzed the utilization of user driven visualization to boost security and user-friendliness of authentication protocols. Planned 2 of protocols that not solely improve the user expertise however also resist difficult

attacks, like the keylogger and malware attacks. Our protocols utilize easy technologies offered in most out-of-the box Smartphone devices. Additionally, we are going to study ways for up the protection and user experience by means that of visualization in different contexts, however not restricted to authentication like visual secret writing and visual signature variation.

REFERENCES

[1] R.Pemmaraju Methods and apparatus for securing keystrokes from being intercepted between the keyboard and a browser. Patent 182,714.

[2] N. Hopper and M. Blum. Secure human identification protocols. In *Proc. of ASIACRYPT*, 2001

[3] DaeHunNyang, Member, IEEE, Aziz Mohaisen, Member, IEEE, Jeonil Kang, Member, IEEE, "**Keylogging-resistant Visual Authentication Protocols**" -IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 11, NOVEMBER 2014

[4] J. Bonneau, C. Herley, P.C. Van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," Proc. IEEE Symp. Security and Privacy (SP), pp. 553-567, 2012.

[5] M. Farb, M. Burman, G. Chandok, and J. McCune, "A. Perrig, "SafeSlinger: An Easy-to-Use and Secure Approach for Human Trust Establishment," Technical Report CMU- CyLab-11-021, Carnegie Mellon Univ., 2011.

[6] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing Shoulder-Surfing by Using Gaze-Based Password Entry," Proc. ACM Third Symp. Usable Privacy and Security (SOUPS), pp. 13-19, 2007.

[7] M. Mannan and P.C. van Oorschot, "Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers," J. Computer Security, vol. 19, no. 4, pp. 703-750, 2011.

[8] H. Moon, H. Lee, J. Lee, K. Kim, Y. Paek, and B.B. Kang, "Vigilare: Toward Snoop-Based Kernel Integrity Monitor," Proc. ACM Conf. Computer and Comm. Security (CCS '12), pp. 28-37, 2012.

[9] D. MRaihi, S. Machani, M. Pei, and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm," RFC 6238, http://www.ietf. org/rfc/rfc6238.txt, 2011.

[10] Q. Yan, J. Han, Y. Li, J. Zhou, and R.H. Deng, "Designing Leakage- Resilient Password Entry on Touchscreen Mobile Devices," Proc. Eighth ACM SIGSAC Symp. Information, Computer and Comm. Security (ASIACCS), pp. 37-48, 2013.

[11] H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda, "Panorama: Capturing System-Wide Information Flow for Malware Detection and Analysis," Proc. ACM Conf. Computer and Comm. Security (CCS), 2007.

