Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 12, December -2017

Security In Healthcare System By Using QR code

[1]Jaid,[2]Piyush,[3]Riyaz,[4]Karan,[5]Prof.Pradip Shewale.

[1]Dr.D.Y.Patil Institute Of Engg. & Technology,Pune,Maharashtra,India
[2]Dr.D.Y.Patil Institute Of Engg. & Technology,Pune,Maharashtra,India
[3]Dr.D.Y.Patil Institute Of Engg. & Technology,Pune,Maharashtra,India
[4]Dr.D.Y.Patil Institute Of Engg. & Technology,Pune,Maharashtra,India
[5]Dr.D.Y.Patil Institute Of Engg. & Technology,Pune,Maharashtra,India

Abstract —*Information is unit associate in growing supply of knowledge generated from hospitals consisting of patient records within the variety of exhausting copies which may be created easier and convenient by mistreatment QR code of the patient details. Our aim is to make a Health-care vascular system which can offer the options like clinical management, patient records, unwellness prediction and generate QR code for each patient as per there updated unwellness data. Keylogging or keyboard capturing is that the activity of recording (or logging) the keys stricken on a keyboard, usually during a incommunicative means in order that the individual utilizing the keyboard is unconscious that their activities area unit being discovered. It likewise has exceptionally authentic uses in investigations of human-computer interaction. There are numerous Keylogging techniques, extending from hardware and package primarily based 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 visualization define will improve the protection 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 had the capability in curing abnormal state of simple use whereas fulfilling demanding security requirements.*

Keywords: *Keylogging,QR code*

I.INTRODUCTION

Medical information square measure associate degree ever growing supply of data generated from hospitals consisting of patient records within the style of onerous copies which might be created easier and convenient by mistreatment QR code of the patient details. Our aim is to make a Health-care vascular system which is able to offer the options like clinical management, patient records, illness prediction and generate QR code for each patient as per there updated illness data. Search illness by mistreatment K-NN algorithmic program and predict illness by mistreatment K-Mean algorithmic program.

Hospitals square measure terribly essential a part of our lives, providing best medical facilities to individuals tormented by numerous diseases. However keeping track of all the activities and records is incredibly error prone. It's conjointly terribly inefficient and time intense method observant the continual increasing population and variety of individuals visiting the hospital. Recording and maintaining the records square measure extremely unreliable and error prone and inefficient. It's conjointly not economically and technically possible to take care of the records on paper. The most aim of project is to produce paper-less up to ninetieth. It conjointly aims at providing low value reliable automation of the prevailing system. There square measure numerous Keylogging techniques, extending from hardware and computer code primarily based methodologies to acoustic examination. As well as human in authentication protocols, whereas guaranteeing, isn't easy in light-weight of their restricted capability of calculation and remembrance. fast Response (QR) codes appear to seem everyplace of late. mistreatment the QR codes is one in every of the foremost intriguing ways in which of digitally connecting shoppers to the net via mobile phones since the mobile phones became a basic necessity issue of everybody. For making QR codes, the admin can enter text into an online browser and can get the QR code generated. whereas QR codes have several benefits that create them very hip, there square measure many security problems and risks that square measure related to them. Running malicious code, stealing users' sensitive data and violating their privacy and fraud square measure some typical security risks that a user can be subject to within the background whereas he/she is simply reading the QR code within the foreground. A security system for QR codes that guarantees each users and generators security considerations are enforced. The project exhibits however careful mental image define will improve the safety moreover because the convenience of authentication.

II. LITERATURE SURVEY

Paper Name:The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes (2012)
Authors:Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajanoy.

Authors are evaluated twenty years of proposals to interchange text passwords for all-purpose user authentication on the online employing a broad set of twenty-five usability, deployability and security advantages that a perfect theme would possibly give. The scope of proposals we tend to survey is additionally in depth, as well as arcanum management software package, federate login protocols, graphical arcanum schemes, psychological feature authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and bioscience. Our comprehensive approach ends up in key insights concerning the problem of substitution passwords. Not solely will no identified theme likened to providing all desired benefits: none even retains the total set of advantages that heritage passwords already give. particularly, there's a large vary from schemes giving minor security advantages on the far side heritage passwords, to those giving important security advantages reciprocally for being additional pricey to deploy or harder to use. We tend to conclude that several tutorial proposals have didn't gain traction as a result of researchers seldom contemplate a sufficiently big selection of real-world constraints. On the far side our analysis of current schemes, our framework provides AN analysis methodology and benchmark for future net authentication proposals.

Paper Name: SafeSlinger: Easy-to-Use and Secure Public-Key Exchange (2011)
Authors: M Farb, Yue-Hsun Lin, Tiffany Hyun-Jin Kim, Jonathan McCune, A PerrigDescription: Users often expertise a crisis of confidence on the net. Is that email or instant message really originating from the claimed individual? Such doubts square measure usually resolved through a leap of religion, expressing the desperation and helplessness of users. To ascertain a secure basis for on-line communication, we tend to propose SafeSlinger, a system investing the proliferation of smartphones to modify folks to firmly and in private exchange their public keys. Through the changed authentic public keys, Safe- thrower establishes a secure channel providing secrecy and legitimacy, that we tend to use to support secure electronic communication and file exchange. SafeSlinger additionally provides associate API for mercantilism applications' public keys into a user's contact info. By throw entire contact entries to others, we tend to propose secure introductions, because the contact entry includes the SafeSlinger public keys similarly as alternative public keys that were foreign.

Paper name: Leveraging Personal Devices for Stronger Password Authentication(2011).

Authors:Mohammad Mannan and P.C. van Oorschot

Description: Internet authentication for standard end-user transactions, like on-line banking and e-commerce, continues to be dominated by passwords entered through end-user PCs. Most users still like (typically untrusted) PCs over smaller personal devices for actual transactions, thanks to usability options associated with keyboard and screen size. But most such transactions and their underlying protocols are at risk of attacks as well as keylogging, phishing, and pharming. we tend to propose Mobile word Authentication (MP-Auth) to counter such attacks, that cryptographically separates a user's long secret input from the consumer computer, and offers dealing integrity. The computer continues to be used for many of the interaction however has access solely to temporary secrets, whereas the user's long secret is input through an freelance personal device, e.g., a radiophone that makes it out there to the computer solely once secret writing underneath the supposed far-end recipient's public key. MP-Auth expects users to input passwords solely to a private device, and be alert whereas confirming transactions from the device. To facilitate a comparison to MP-Auth, we tend to additionally give a comprehensive survey of internet authentication techniques that use a further issue of authentication; this survey is also of freelance interest.

4. Designing Leakage-Resilient Password Entry onTouchscreen Mobile Devices (2013).
Author: Qiang Yany, Jin Hanz, Yingjiu Liy, Jianying Zhouz, Robert H. Dengy.
Description: Touchscreen mobile devices are becoming commodities as the wide adoption of pervasive computing. These devices allow users to access various services at anytime and anywhere. In order to prevent unauthorized access to these services, passwords have been pervasively used in user authentication. However, password-based authentication has intrinsic weakness in password leakage. This threat could be more serious on mobile devices, as mobile devices are widely used in public places. Most prior research on improving leakage resilience of password entry focuses on desktop computers, where specific restrictions on mobile devices such as small screen size are usually not addressed. Meanwhile, additional features of mobile devices such as touch screen are not utilized, as they are not available in the traditional settings with only physical keyboard and mouse. In this paper, we 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. It is also designed to retain most benefits of legacy passwords, which is critical to a scheme intended for practical use. The usability of Cover- Pad is evaluated with an extended user study which includes additional test conditions related to time pressure, distraction, and mental workload. These test conditions simulate common situations for a password entry scheme used on a daily basis, which have not been evaluated in the prior literature. The results of our user study show the impacts of these test conditions on user performance as well as the practicability of the proposed scheme.

III. EXISTING SYSTEM

Whenever a user varieties in her watchword during a bank's signin box, the keylogger intercepts the watchword. The threat of such keyloggers is pervasive and might be gift each in personal pcs and public kiosks; there area unit perpetually cases wherever it's necessary to perform money transactions employing a public computer though the most important concern is that a user's watchword is probably going to be purloined in these computers. Even worse, keyloggers, typically root kitted, area unit arduous to sight since they'll not show up within the task manager method list.

DISADVANTAGOUS OF EXISTING SYSTEM

- It is non-Security for stored data.
- Security level is low.
- QR code is not encrypted which is less secure.
- It doesn't challenges the paperless work.

IV PROPOSED SYSTEM

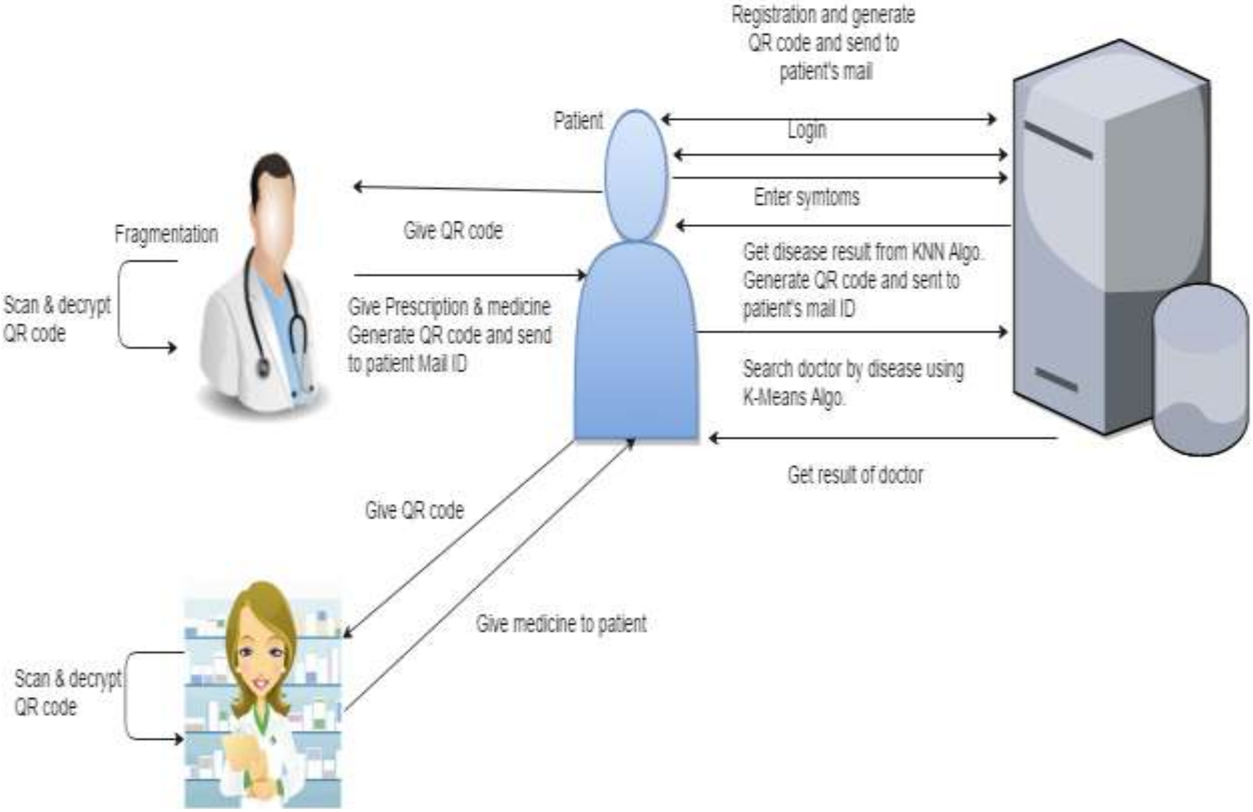
In order to shorten the paperless work procedures when a patient visiting regularly or seen in the emergency case, we will be retrieving their information which is scanned with the help of a QR Code containing a link of the victim's emergency information stored in database.

When patients first visits to hospital, perform registration process with system. At the time of login there are two step one is password based and another is OTP based, in password based he will enters the his username/ email with password. In second step the system will ask the OTP displayed the normal keypad which is visualized and respected OTP and the actual pattern of that keypad is sent to users email ID upon successfully entering the correct email and password of that user.

Upon successful login, user will his check up details and submits and system will generate the QR of that users information and that QR will be keep at admins records and user will get the ID for his his record. When user visits the hospital he will tell only his ID and admin will scan repected ID's QR code and proceeds accordingly.

If any change in users details then he will login to his account and do changes then system will generate new QR code. And next time admin will use that newly generated QR code.

The admin or hospital person who handling this system can view all the details of all the users registered with that system as he is only authorized person


Registration and generate QR code and send to patient's mail
Patient
Login
Enter symtoms
Get disease result from KNN Algo. Generate QR code and sent to patient's mail ID
Search doctor by disease using K-Means Algo.
Get result of doctor
Fragmentation
Scan & decrypt QR code
Give QR code
Give Prescription & medicine Generate QR code and send to patient Mail ID
Give QR code
Give medicine to patient
Scan & decrypt QR code

ADVANTAGEOUS OF PROPOSED SYSTEM

1. A novel QR code Strategy based on encryption technique which can challenge the existing QR code strategy.
2. The system implementations in the form of Android applications which demonstrate the usability of our protocols in real-world deployment settings.
3. To generate QR code for every patient as per there disease the system takes less time.
4. Every interaction between the user and an intermediate helping device is visualized using a Quick Response (QR) code.
5. It Support reasonable Image security and usability and appears to fit well with some practical applications for improving online security.
6. Patient no need to visit personally to the physician or at medical store.

III.CONCLUSION AND FUTURE SCOPE

We proposed health care system for hospital for this we are using K-NN algorithms. We generate QR code for every patient. We also proposed and analyzed the use of user driven visualization to improve security and user-friendliness of authentication protocols.Proposed two of protocols that not only improve the user experience but also resist challenging attacks, such as the keylogger and malware attacks. Our protocols utilize simple technologies available in most out-of-the box Smartphone devices. In addition, we will study methods for improving the security and user experience by means of visualization in other contexts, but not limited to authentication such as visual decryption and visual signature verification.

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.