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

QR Code Based Healthcare System

[1]Maithili N. Palshikar, [2]Priyanka S. Mane, [3]Aishwarya S. Dhore, [4]Bhushan P. Kalegore, [5]Prof. Sushma Shinde

[1]Siddhant College of Engineering, Sudumbare, Department of Computer Engineering
[2]Siddhant College of Engineering, Sudumbare, Department of Computer Engineering
[3]Siddhant College of Engineering, Sudumbare, Department of Computer Engineering
[4]Siddhant College of Engineering, Sudumbare, Department of Computer Engineering
[5]Siddhant College of Engineering, Sudumbare, Department of Computer Engineering

Abstract--- *Medical information area unit AN ever growing supply of data generated from hospitals consisting of patient records within the variety of arduous copies which might be created easier and convenient by mistreatment QR code of the patient details. Our aim is to create a Health-care vascular system which is able to offer the options like clinical management, patient records, wellness prediction and generate QR code for each patient as per there updated wellness data. Keylogging or keyboard capturing is that the activity of recording (or logging) the keys stricken on a keyboard, commonly during a incommunicative manner so 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 a unit numerous Keylogging techniques, extending from hardware and software package 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. We tend to exhibit however careful image define will improve the safety additionally because the convenience of authentication. We tend to propose to visual authentication protocols: one may be a one-time-password protocol, and also the different may be a password-based authentication protocol. Our approach for real arrangement: we tend to have the capability attain to an abnormal state of simple use whereas fulfilling tight security wants.*

Keywords--- *Keylogging, QR Code, Medical Data, Health-care Portal system.*

I. INTRODUCTION

Visual authentication and Secure Authentication System for Patient knowledge Management Medical knowledge square measure an ever growing supply of data generated from hospitals consisting of patient records within the variety of arduous copies which may be created easier and convenient by victimization QR code of the patient details. Our aim is to make an aid vascular system which is able to give the options like clinical management, patient records, illness prediction and generate QR code for each patient as per there updated illness info. Search illness by victimization Naïve mathematician rule and predict illness to patient. Hospitals square measure terribly essential a part of our lives, providing best medical facilities to individuals full of varied diseases. However keeping track of all the activities and records is incredibly error prone. It additionally terribly inefficient and time intense method perceptive the continual increasing population and range of individuals visiting the hospital. Recording and maintaining the records square measure extremely unreliable and error prone and inefficient. It’s additionally not economically and technically possible to keep up the records on paper. The most aim of project is to supply paper-less up to ninetieth. It additionally aims at providing low value reliable automation of the prevailing system. There square measure varied 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 lightweight of their restricted capability of calculation and remembrance. Fast Response (QR) codes appear to seem everyplace recently. victimization the QR codes is one amongst the foremost intriguing ways in which of digitally connecting customers to the web via mobile phones since the mobile phones became a basic necessity factor of everybody. For making QR codes, the admin can enter text into an internet 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 info 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 issues are enforced. The project exhibits however careful mental image define will improve the safety additionally because the convenience of authentication.

II. LITERATURE SURVEY

2.1. Paper Name: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes (2012) [1]
Authors: Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajanoy.
Description: Authors are evaluated two decades of proposals to interchange text passwords for all-purpose user authentication on the online employing a broad set of twenty-five usability, deploy ability and security advantages that a perfect theme may offer. The scope of proposals we have a tendency to survey is additionally in depth, as well as word management code, federate login protocols, graphical word schemes, psychological feature authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometry. Our comprehensive approach ends up in key insights concerning the issue of replacement passwords. Not solely will no best-known theme equated to providing all desired benefits: none even retains the total set of advantages that heritage passwords already offer. specially, there's a large vary from schemes providing minor security advantages on the far side heritage passwords, to those providing important security advantages reciprocally for being a lot of pricey to deploy or tougher to use. we have a tendency to conclude that a lot of tutorial proposals have didn't gain traction as a result of researchers seldom take into account a sufficiently big selection of real-world constraints. on the far side our analysis of current schemes, our framework provides associate analysis methodology and benchmark for future net authentication proposals.

2.2. Paper Name: SafeSlinger: Easy-to-Use and Secure Public-Key Exchange (2011) [2]
Author: M Farb, Yue-Hsun Lin, Tiffany Hyun-Jin Kim, Jonathan McCune, A Perrig

Description: Users frequently expertise a crisis of confidence on the net. Is that email or instant message actually originating from the claimed individual? Such doubts square measure normally resolved through a leap of religion, expressing the desperation and helplessness of users. to determine a secure basis for on-line communication, we have a tendency to propose SafeSlinger, a system investing the proliferation of smartphones to change individuals to firmly and in private exchange their public keys. Through the changed authentic public keys, Safe- thrower establishes a secure channel giving secrecy and credibility, that we have a tendency to use to support secure electronic messaging and file exchange. SafeSlinger conjointly provides associate API for mercantilism applications' public keys into a user's contact info. By throw entire contact entries to others, we have a tendency to propose secure introductions, because the contact entry includes the SafeSlinger public keys furthermore as alternative public keys that were foreign.

2.3. Paper Name: Leveraging Personal Devices for Stronger Password Authentication (2011) [3]
Author: Mohammad Mannan and P.C. van Oorschot
Description: Internet authentication for fashionable 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, as a result of usability options associated with keyboard and screen size. but most such transactions and their underlying protocols area unit susceptible to attacks together with keylogging, phishing, and pharming. we have a tendency to propose Mobile watchword Authentication (MP-Auth) to counter such attacks, that cryptographically separates a user's long-run secret input from the consumer computer, and offers group action integrity. The computer continues to be used for many of the interaction however has access solely to temporary secrets, whereas the user's long-run secret is input through associate freelance personal device, e.g., a mobile phone that makes it offered to the computer solely when encoding underneath the supposed far-end recipient's public key. MP-Auth expects users to input passwords solely to a private device, and be wakeful whereas confirming transactions from the device. To facilitate a comparison to MP-Auth, we have a tendency to additionally give a comprehensive survey of internet authentication techniques that use a further issue of authentication; this survey could also be of freelance interest.

2.4. Paper Name: Designing Leakage-Resilient Password Entry on Touchscreen Mobile Devices (2013) [4]
Author: Qiang Yany, Jin Hanz, Yingjiu Liy, Jianying Zhouz, Robert H. Dengy.
Description: Touchscreen mobile devices are getting commodities because the wide adoption of pervasive computing. These devices enable users to access varied services at anytime and anyplace. So as to forestall unauthorized access to

those services, passwords are pervasively utilized in user authentication. However, secret-based authentication has intrinsic weakness in password leak. This threat might be a lot of serious on mobile devices, as mobile devices area unit wide utilized in public places. Most previous analysis on up leak resilience of secret entry focuses on desktop computers, wherever specific restrictions on mobile devices like tiny screen size area unit typically not addressed. Meanwhile, extra options of mobile devices like bit screen don't seem to be utilized, as they're not accessible within the ancient settings with solely physical keyboard and mouse. During this paper, we have a tendency to propose a user authentication theme named Cover- Pad for secret entry on touchscreen mobile devices. CoverPad improves leak resilience by safely delivering hidden messages that break the correlation between the underlying secret and therefore the interaction info noticeable to associate antagonist. It's additionally designed to retain most edges of gift passwords, that is important to a theme supposed for sensible use. The usability of Cover- Pad is evaluated with associate extended user study which has extra check conditions associated with time pressure, distraction, and mental employment. These check conditions simulate common things for a secret entry theme used on a day to day, that haven't been evaluated within the previous literature. The results of our user study show the impacts of those check conditions on user performance yet because the of the planned theme.

III. EXISTING SYSTEM

Whenever a user sorts in her secret in a very bank's register box, the keylogger intercepts the secret. The threat of such keyloggers is pervasive and might be gift each in personal pcs and public risks; there are a unit invariably cases wherever it's necessary to perform monetary transactions employing a public computer though the most important concern is that a user's secret is probably going to be purloined in these computers. Even worse, keyloggers, usually root kitted, area unit arduous to observe since they'll not show up within the task manager method list. Additionally the paper work is simply too abundant. The any user or patients need to carry all the main points at the time of treatment. The prediction of sickness isn't excellent.

3.1 Disadvantages of Existing System

1. It is non-Security for stored data.
2. Security level is low.
3. QR code is not encrypted which is less secure.
4. 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 checkup 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 respected ID's QR code and proceeds accordingly.

If any change in user's 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.

4.1 Advantages 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 needs to visit personally to the physician or at medical store.

V. SYSTEM ARCHITECTURE

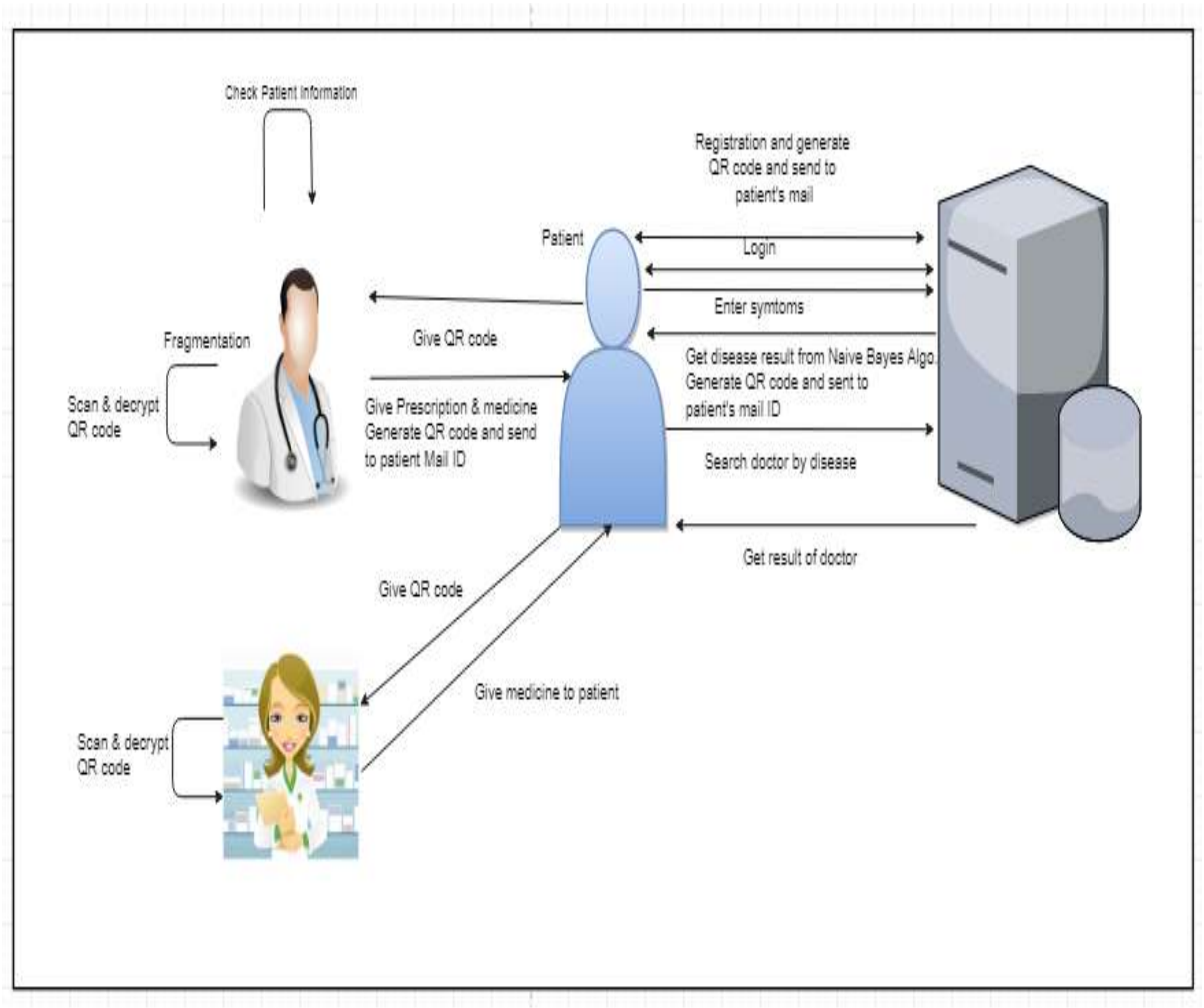
Check Patient Information
Registration and generate QR code and send to patient's mail
Patient
Login
Enter symtoms
Fragmentation
Give QR code
Scan & decrypt QR code
Get disease result from Naive Bayes Algo. Generate QR code and sent to patient's mail ID
Give Prescription & medicine Generate QR code and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

Figure 1. System Architecture of Proposed System

1. Patient:

A. Registration

✓ The patient will register to the system with normal information.

✓ At the time of registration patient will enter valid Email-ID and receives QR code on his Email-ID which in encrypted format.

B. Login

✓ For login to the system, patient will enter the Email and password, if entered details are correct then the system will redirect him to home page otherwise it will shows an error message.

After Login:

1. Patient will enter the symptoms.
2. Then patient get disease result and generate QR code and sent to patients Mail ID.
3. Patient will search for doctor as per disease shown by system.
4. Patient will get result of doctors.

C. Logout

Patient logout the account from system.

2. Doctor

A. Registration

✓ Doctor will register to the system with normal information.

B. Login into Scanner.

✓ Patient gives QR code to the doctor which is received in his mail ID.

✓ Doctor login into scanner.

After Login:

1. Doctor scans and decrypts the QR code.
2. Then gives prescription and medicine in QR code format and send to patient Mail ID.
3. The alert will be generated and send to user on his profile regarding prescription.

- **The patient info apps (this is accessible to doctor only)**

- Contains patients list
- Patient summary
- Lab results
- Medication list,
- Clinical notes
- Vital signs
- Allergies
- Current treatment information
- Doctor notes.

C. Logout

Doctor Logout the account from system.

3. Pharmacist

A. **Login into Scanner.**

✓ Patient gives prescription QR Code which is received in his mail ID.

✓ Pharmacist login into scanner.

After Login:

1. Pharmacist scans and decrypts the QR code.
2. Then give medicine to patient.

B. Logout

Pharmacist Logout the account from system.

VI. CONCLUSION

We proposed health care system for hospital for this we are using Naïve Bayes and Blowfish algorithms. We generate QR code for every patient. We proposed and analyzed the use of user driven visualization to improve security and user-friendliness of authentication approaches. Proposed two of conventions 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] 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.

[2] 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.

[3] 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.

[4] 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.