Healthcare System By Using QR Code Strategy

[1]Rushabh jain, [2]Swapnil khade, [3]Nikhil kothawale, [4]Aditya patil, [5]Prof. Sarika Zaware

Departmentof computer engineering. AISSMS Institute of Information technology, Pune, Maharashta, India.

Abstract: *Medical information are Associate in Nursing ever growing supply of data generated from hospitals consisting of patient records within the variety of onerous copies which may be created easier and convenient by victimisation 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, sickness prediction and generate QR code for each patient as per there updated sickness data. Key-logging or keyboard capturing is that the activity of recording (or logging) the keys affected on a keyboard, commonly in a very uncommunicative manner so the individual utilizing the keyboard is unconscious that their activities are being ascertained. It likewise has exceptionally authentic uses in investigations of human-computer interaction. There are varied Key-logging techniques, extending from hardware and computer code based mostly methodologies to acoustic examination. Together with human in authentication protocols, whereas guaranteeing, isn't easy in light-weight of their restricted capability of calculation and remembrance. we have a tendency to exhibit however careful image define will improve the protection additionally because the convenience of authentication. We have a tendency to propose 2 visual authentication protocols: one may be a one-time- word protocol, and also the alternative may be a password-based authentication protocol. Our approach for real arrangement: we have a tendency to have the capability attain to Associate in Nursing abnormal state of easy use whereas fulfilling rigorous security requirements.*

1. INTRODUCTION

Visual Associate in Nursing Secure Authentication System for Patient information Management medical information are an ever growing supply of data generated from hospitals consisting of patient records within the variety of onerous copies which may be created easier and convenient by victimisation 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, sickness prediction and generate QR code for each patient as per there updated sickness data. Search sickness by victimisation Naïve Thomas Bayes rule and predict sickness of patient.

Hospitals are terribly essential a part of our lives, providing best medical facilities to folks plagued by varied diseases. However keeping track of all the activities and records is incredibly error prone. It’s conjointly terribly inefficient and time overwhelming method observant the continual increasing population and variety of individuals visiting the hospital. Recording and maintaining the records are 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 supply paper-less up to ninetieth. It conjointly aims at providing low price reliable automation of the prevailing system. There are varied Key-logging techniques, extending from hardware and computer code based mostly methodologies to acoustic examination. Together with 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 look everyplace of late. victimisation the QR codes is one amongst the foremost intriguing ways that of digitally connecting customers 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 internet browser and can get the QR code generated. Whereas QR codes have several benefits that build them highly regarded, there are many security problems and risks that are related to them. Running malicious code, stealing users’ sensitive data and violating their privacy and fraud are some typical security risks that a user may well 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 image define will improve the protection additionally because the convenience of authentication.

2. PROBLEM DEFINITION

In this system the health data is keep on the third party server. There’s no cryptography and coding of health data thus there's chance of non-public health data may be uncovered to unauthorized parties and third party servers. Single owner system, during which no policy management for file access. Adding the classes isn't doable thus hint is additionally accessed by every type of users.

a. There are varied Key-logging techniques, extending from hardware and computer code based mostly methodologies to acoustic examination. together with human in authentication protocols, whereas guaranteeing, isn't easy in light-weight of their restricted capability of calculation and remembrance.

b. 2 approaches for authentication are used one is word-based authentication and one-time password based mostly authentication that uses image by technique for exaggerated reality to relinquish each high security and high convenience.

c. Model utilization as humanoid applications that demonstrate the convenience of our conventions in true organization settings.

3. SCOPE

We will study ways for raising the protection and user expertise by means that of image in different contexts, however not restricted to authentication like visual coding and visual signature verification. Finally, reportage on user studies which will have the benefit of a good preparation and acceptance of our protocols would be a parallel future work to think about similarly. we tend to analyzed the utilization of user- driven image to boost security and user-friendliness of authentication protocols. Moreover, we've shown 2 realizations of protocols that not solely improve the user expertise however conjointly resist difficult attacks, like the key-logger and malware attacks. Our protocols utilize easy technologies on the market in most out-of- the- box sensible phone devices. We tend to developed mechanical man application of an example of our protocol and demonstrate its practicability and potential in real-world preparation and operational settings for user authentication.

Our work so opens the door for many different directions that we might prefer to investigate as a future work. 1st of all, our arrange is to implement our protocol on the sensible glasses like the Google glass, and conduct the user study. Second, we tend to commit to investigate the look of different protocols with a lot of demanding performance necessities victimization equivalent tools provided during this work. additionally, we'll study ways for rising the protection and user expertise by means that of image in different con- texts, however not restricted to authentication like visual coding and visual signature verification.

4. OBJECTIVES

1. To point out however image will improve security similarly as convenience by proposing 2 visual verification conventions.
2. Our techniques area unit safe to variety of the testing attacks like shoulder surfing attack at the time of login authentication.
3. Example implementations within the kind of mechanical man applications that demonstrate the usability of our protocols in real-world preparation settings.
4. To get QR code for each patient anamnesis.
5. To look near Doctor of the offer symptoms.
6. To scan the QR code of each patient by victimization scanner which is able to be operated on mechanical man phone and also the QR code are scanned by doctor.

5. MOTIVATION

There are unit some application's on the market for doctor and patient however there's no such application that helps to optimize upshot of diseases, technique to verify the diseases of patients. For this we tend to area unit generating a QR code as per there malady. Conjointly patient seeks for doctor by victimization Naïve Bayes rule and malady prediction to the patient. Key-logging exhibits AN extraordinary take a look at to security supervisors. Dissimilar to customary worms and viruses, certain sorts of key-loggers area unit everything except tough to get. Key-loggers area unit a sort of malware that malignantly track client info from the comfort trying to recuperate individual and personal info. Growing machine use for essential business and individual activities victimization the web has created possible treatment of Key-logging basic..

6. LITERATURE SURVEY

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)". [1] Authors have been evaluated two decades of proposals to replace text passwords for general-purpose user authentication on the web using a broad set of twenty-five usability, deployability and security benefits that an ideal scheme might provide. The scope of proposals we survey is also extensive, including password management software, federated login protocols, graphical password schemes, cognitive authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometrics. Our comprehensive approach leads to key insights about the difficulty of replacing passwords. Not only does no known scheme come close to providing all desired benefits: none even retains the full set of benefits that legacy passwords already provide. In particular, there is a wide range from schemes offering minor security benefits beyond legacy passwords, to those offering significant security benefits in return for being more costly to deploy or more difficult to use. We conclude that many academic proposals have failed to gain traction because researchers rarely consider a sufficiently wide range of real-world constraints. Beyond our analysis of current schemes, our framework provides an evaluation methodology and benchmark for future web authentication proposals.

Mohammad Mannan and P.C.van Oorschot,"Leveraging Personal Devices for Stronger Password Authentication. (2011)" [2] Internet authentication for popular end-user transactions, such as online banking and e-commerce, continues to be dominated by passwords entered through end-user PCs. Most users continue to prefer (typically untrusted) PCs over smaller personal devices for actual transactions, due to usability features related to keyboard and screen size. However most such transactions and their underlying protocols are vulnerable to attacks including key-logging, phishing, and pharming. We propose Mobile Password Authentication (MP-Auth) to counter such attacks, which cryptographically separates a user's long-term secret input from the client PC, and offers transaction integrity. The PC continues to be used for most of the interaction but has access only to temporary secrets, while the user's long-term secret is input through an independent personal device, e.g., a cellphone which makes it available to the PC only after encryption under the intended far-end recipient's public key. To facilitate a comparison to MP-Auth, we also provide a comprehensive survey of web authentication techniques that use an additional factor of authentication; this survey may be of independent interest.

M Farb, Yue-Hsun Lin, Tiffany Hyun-Jin Kim, Jonathan McCune, A Perrig, "Safe Slinger: Easy-to- Use and Secure Public-Key Exchange (2011)" [3] Users regularly experience a crisis of confidence on the Internet. Is that email or instant message truly originating from the claimed individual? Such doubts are commonly resolved through a leap of faith, expressing the desperation and helplessness of users. To establish a secure basis for online communication, we propose Safe Slinger, a system leveraging the proliferation of smart phones 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. Safe Slinger also provides an API for importing applications' public keys into a user's contact information. By slinging entire contact entries to others, we propose secure introductions, as the contact entry includes the Safe Slinger public keys as well as other public keys that were imported.

Qiang Yany, Jin Hanz, Yingjiu Liy, Jianying Zhouz, Robert H. Dengy.[4] 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 touch screen mobile devices. Cover Pad 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.

EXISTING SYSTEM

1) Whenever a user types in her password in a bank's sign in box, the key-logger intercepts the password.

2) The threat of such key-loggers is pervasive and can be present both in personal computers and public kiosks; there are always cases where it is necessary to perform financial transactions using a public computer although the biggest concern is that a user's password is likely to be stolen in these computers.

3) Even worse, key-loggers, often root kitted, are hard to detect since they will not show up in the task manager process list.

DISADVANTAGOUS 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.

7. 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 are 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 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.

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.

NAÏVE BAYES ALGORITHM

1. Introduction

A Naive Bayes classifier is a simple probabilistic classifier based on applying Bayes theorem (from Bayesian statistics) with strong (naive) independence assumptions. A more descriptive term for the underlying probability model would be independent feature model. In simple terms, a naive Bayes classifier assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature.

For example, a fruit may be considered to be an apple if it is red, round, and about 4&quot; in diameter. Even if these features depend on each other or upon the existence of the other features, a naive Bayes classifier considers all of these properties to independently contribute to the probability that this fruit is an apple. Depending on the precise nature of the probability model, naive Bayes classifiers can be trained very efficiently in a supervised learning setting. In many practical applications, parameter estimation for naive Bayes models uses the method of maximum likelihood; in other words, one can work with the naive Bayes model without believing in Bayesian probability or using any Bayesian methods.

An advantage of the naive Bayes classifier is that it only requires a small amount of training data to estimate the parameters (means and variances of the variables) necessary for classification. Because independent variables are assumed, only the variances of the variables for each class need to be determined and not the entire covariance matrix.

A) AES ALGORITHM

In the implementation of this AES-256 algorithm has a plaintext of 128 bits and key of 256 bits size. The number of rounds of operations in AES- 256 is 14. The key generation process of AES 256 is different from other AES algorithms. The AES-256 algorithm is composed of three main parts: Cipher, Inverse Cipher and Key Expansion. Cipher converts data to an unintelligible form called cipher text while Inverse Cipher converts data back into its original form called plaintext. Key Expansion generates a Key Schedule that is used in Cipher and Inverse Cipher procedure. Cipher and Inverse Cipher are composed of specific number of rounds For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations:

1) Byte substitution using a substitution table (S-box)

2) Shifting rows of the State array by different offsets

3) Mixing the data within each column of the State array

4) Adding a Round Key to the State

The Cipher transformations can be inverted and then implemented in reverse order to produce a straightforward Inverse Cipher for the AES algorithm. The individual transformations used in the Inverse Cipher.

1) Inverse Shift Rows

2) Inverse Sub Bytes

3) Inverse Mix Columns

4) Add Round Key

The AES inverse cipher core consists of a key expansion module, a key reversal buffer, an initial permutation module, a round permutation module and a final permutation module. The key reversal buffer first store keys for all rounds and the presents them in reverse order to the rounds. The round permutation module will loop maternally to perform 14 iterations (for 256 bit keys).

B) K-nearest neighbors (KNN) algorithm

Here is step by step on how to compute K-nearest neighbors KNN algorithm:

1. Determine parameter K = number of nearest neighbors

2. Calculate the distance between the query-instance and all the training samples

3. Sort the distance and determine nearest neighbors based on the K-th minimum distance

4. Gather the category Y of the nearest neighbors

5. Use simple majority of the category of nearest neighbors as the prediction value of the query instance Time complexity and optimality of kNN

c) Architecture Design

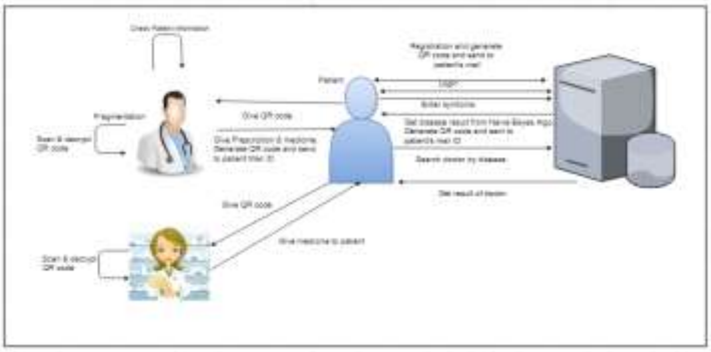
Check Patient information
Registration and generate QR code and send to patient's mail
Patient
Login
Enter symptoms
Prescription
Give QR code
Get disease result from Naive Bayes Algo
Generate QR code and sent to patient's mail ID
Scan & decrypt QR code
Give Prescription & medicine Generate QR code and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

Fig 1: *Architecture Design*

8. CONCLUSION

We planned health care system for hospitals for this we tend to are exploitation AES and Naïve mathematician algorithms. We tend to generate QR code for each patient. We tend to planned and analyzed the employment of user driven mental image to enhance security and user-friendliness of authentication approaches. Planned 2 conventions that not solely improve the user expertise however conjointly resist difficult attacks, like the key-logger and malware attacks. Our protocols utilize straightforward technologies accessible in most out-of- the box Smartphone devices. Additionally, we'll study strategies for raising the safety and user expertise by means that of mental image in different contexts, however not restricted to authentication like visual cryptography and visual signature verification.

REFERENCES

[1] R.Pemmaraju Methods and apparatus for securing keystrokes from being interceptedbetween 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.

[12] Chen, Chia-Hsin Owen, et al. &quot;GAnGS: gather, authenticate&#39;n group securely.&quot; Proceedings of the 14th ACM international conference on Mobile computing and networking. ACM, 2008.