Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN : 2348-4470
p-ISSN : 2348-6406

International Journal of Advance Engineering and Research Development

Special Issue on Recent Trends in Data Engineering

Volume 4, Special Issue 5, Dec.-2017

The Automated System For General Administration Using QR Code

Prof.D.S.Zingade[1], Swati Shirsat[2], Ankita Varade[3], Mansi Sable[4], Vishal.Jangade[5]

[1] *Computer Department, AISSMS Institute of Information Technology*
[2] *Computer Department, AISSMS Institute of Information Technology*

Abstract —*The keystroke logging is referred to as keylogging in which the steokes of keyboard are captured, which means that the keys pressed on the keyboard are recorded. Except this the action of the person are observed and which are unknown to the person. There are various kinds of rootkits which are present in PC's and the user behaviour is been observed which make PC's untrusted device. When we need to focus on large network computer security is main subject of concern. There are large number of keylog methods that rangesfrom hardware and software methods to acoustic analysis. Fortunately there are preventive measures to search and destroy keyloggers or keep them at bay these we can keep away ourself from malware attacks as well as shoulder suffering attacks we implemented sophisticated method for security using QR code. Here we have demonstrated two protocols for visual authentication purpose which are term as OTP based protocol and password based protocol. Here we show how visualization can improve security as well as convenience by proposing two visual verification convention, one for password based authentication other one is one time password.*

Keywords- *Keylogging; Authentication; QR Code; Two Protocals.*

INTRODUCTION

Computer security is the crucial factor which is to be considered with respective to large networks. Computer security is also known as cyber security, is nothing but securing the information from thefts or any other malware attack. A keylogger is a type of software that is considered as spyware which has the ability to record the keystroke after pressing the keys. Any e-mail information and messages can be recorded at anytime by the keylogger. Keylogger tool is mostly used by the employers who make use of computer in banking system, hospitality to make sure that their password or another information is secured. Keyloggers are of different types: hardware and software keylogger devices, monitors the physical keystroke of computer users. There are some keyloggers who can record the URL sites and also the mail address. In the act of keylogger. The password of the user is being known whenever the person sign-in for any purpose. Such a keyloggers are also present in personal computers. There are many situation where we have to use public computers for transaction or any other purpose, so in this case the password is most likely to be stolen, to avoid this act of hacking password. We can propose a visual keyboard, which consists of shuffled keypad. Whenever a user sign's in shoulder suffering attack may occur to prevent this attack. Shuffled visual keypad technique is proposed. There are many other technique to prevent this attack. In this paper, we have proposed a system which make use of two protocols: one is one time password and other is password based authentication. We have also shown visualization can improve security.

OBJECTIVE

New scheme for detecting QR code generation.
To identify user information and then decrypt QR and send to particular user.
To reduce time required for verified certificate.
Minimize the effort required for filling the form

LITERATURE SURVEY

Designing Leakage-Resilient Password Entry On Touchscreen Mobile Devices, AuthorQ. Ya. Han, Y. Li, J. Zhou, and R.H. Deng n, J,2013In this paper, we propose a user authentication scheme named cover-pad for password entry on touchscreen mobile devices.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Authentication Schemes, Authors J. Bonneau, C. Herley, P.C. Van Web Oorschot, and F. Stajano 2012Authors have evaluated proposal for replacement of password for general purpose user authentication on the internet using a broadset. Our system protocol methodology and it set a high milestone for future work authentication.

SafeSlinger: An Easy-to-Use and Secure Approach for Human Trust Establishment, Authors M. Farb, M. Burman, G. Chandok, and J. McCune, A. Perrig 2011Authors have proposed safeslinger system where the public keys can be exchanged securely and privately by the people on the basis of online communication. Secured channel is been provided

@IJAERD-2017, All rights Reserved

by the safeslinger which offers us secrecy and authenticity which is been used by users for file exchanged and secured messaging.

GAnGS: Gather, Authenticate's Group Securely, Authors Chen, Chia-Hsin Owen, et al. 2008. In this paper, they present Gangs the system was implemented where information between mobile devices for exchanging data securely at the same location when they are physically present.

Short Signatures Without Random Oracles, authors Dan Boneh, Xavier Boyen. Authors have described, a short signature scheme under a choosen message attack which is unforgettable without using random oracles. The complexity assumption scheme is been used for the security purpose which is strong Diffie-hellman assumption.

PROPOSED METHODOLOGY

Step-1: Registration Process:
In this stage, the user will fill an online form provided by the organization on their website. This online form will be consisting of all required details for the database. Information stored in database and displayed to user.

Step 2:Login processs keylogger:
In this stage user will login using two type:first one is simple way and second way we have to login using keylogger in that keylogging we generate visual keypad using that visual keypad we will enter our password and authnicate user After successfully filling the online form, the information will be stored in the database and the webpage which will contain all the details of the user will be shown to the user. The database will be stored in the cloud.

Step-3: Generate QR code:
After successful registration of user the QR code is generated by the system. unique 2D QR code will be generated for each user.

Step-4: Sending confirmation mail containing the QR code to the user:
A confirmation mail containing the unique 2D QR code and secrete key which is used to decrypt that QR code of the user will be sent to the user after the QR code is generated successfully.

Step-5: Scan QR code:
A smartphone application will be used for scanning the QR code. before scanning the QR code, authorized login will be provided to the particular authorities

Step-6: Link retrieval and display link:
After scanning the QR code, data will be retrieved and displayed to the user scanning the QR code.

Step-7 : Display information of the user:
the user have to click on the link and then the download form

SYSTEM ARCHITECTURE

In this system, user will register and then at the time of registration user will be provided username and password. At the time of login OTP will be generated and which will be providedto through the email when the user is going to enter his password during login the shuffle keypad technique will be used and system will generated QR code. to the information filled by the user. This QR code will be send to the user's mail. At the same time the general administration willl scan the QR code of the user and he/she will decrypt and verify the information. After the verification process, the user will be able to download the particular document he/she has requested for.

@IJAERD-2017, All rights Reserved

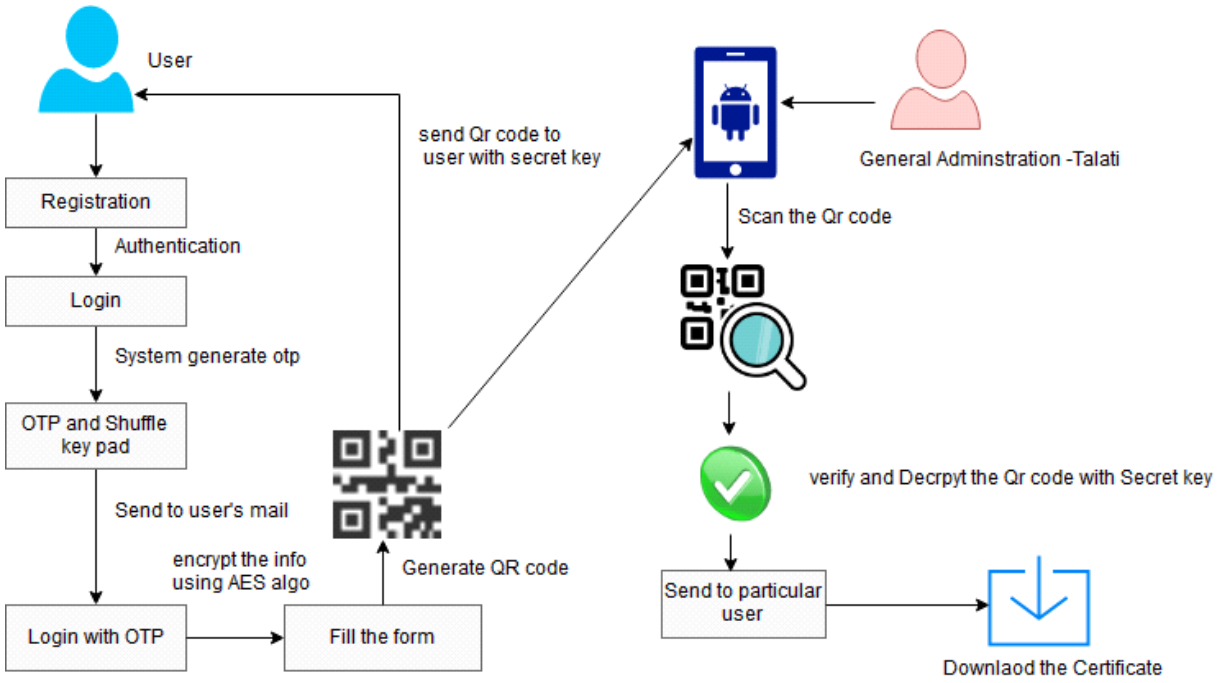

Figure 1.Architecture Diagram

AES ALGORITHM

Initialization
Password, key, Time, salt:string
Time-get_time
Input-password
Key- salt+time
Encryption
Chipertext-AES encrypt(password, key)
Output(chipertext)
Decryption
Key-salt-time
for as much tolerance given time
if key = get_time
key- salt+time
plaintext-AES decrypt(chipertext, key)
end if
end for
Output(plaintext)

CONCLUSION

In this paper, we proposed and analyze the use of two visual authentication protocols, to show how visualization can improve the security and overcome attack using keylogger technique. Moreover, we have shown protocols that only reduces the attacks but also improves the users experience. Here we have used android application for keyloggger and QR code which provides potential and feasibility in real world. For future scope our system can be extended in many direction for the future work.

REFERENCES

[1]4. J. Bonneau, C. Herley, P.C. Van Web Oorschot, and F. Stajano, The Quest to Replace Passwords: A Framework for Comparative Evaluation of Authentication Schemes, Proc. IEEE Symp. Security and Privacy (SP), pp. 553-567, 2012

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

@IJAERD-2017, All rights Reserved

[3] 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.

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

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

[6] Dan Boneh, Xavier Boyen"Short Signatures Without Random Oracles"

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

[8]"Toward Snoop-based Kernel Integrity Monitor"Hyungon Moon,Hojoon LeeJihoon , LeeKihwan Kim, Yunheung Paek,Brent Byunghoon Kang

[9] 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.

[10]"YAGP: Yet Another Graphical Password Strategy" Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu

@IJAERD-2017, All rights Reserved