E-DOCUMENTS WITH APPLIED QR CODE AND KEY LOGGING SECURITY

Aditya Sanjay Deshmukh*1, Ajinkya Rajendra Gawade*2

*1,2SVPM COE, Malegaon, India.

ABSTRACT

Project aims to implementing the E-doc system, with the help of applied QR Code and Key logging security System allows user to request for any document without being physically visiting the government offices. User just need to get registered in our system, by filling the registration form. And later sign in using the User Id, Password, OTP and Shuffle Keypad. Once logins is success then user need to raise the request by filling form like Domicile, Caste Certificate, Non-Creamy layer etc. Then the information is reached to the regional office in the form secure QR Code. As a part of system, we have developed an android application, which is used by authorized person from regional office to scan the QR Code (Info sent by user for requesting Document). If authorized officer found the information as per the set criteria, then he approves the request or else he deny it. It the request is approved then the requested document gets generated in the form of pdf and is sent back to the user, so that he can download it. The entire process takes place virtually.

I.   INTRODUCTION

In our country various certificates like caste, noncreaky layer, income etc. are issued by the concerned State Government authorized authorities. Each State Government/UT administration has laid down its own procedure for issuance of certificates. Efforts are being made to standardize the format of the certificate as far as possible. Wherever feasible, efforts are made to issue. the certificate in bilingual including the language (s) of the State. So far, all the certificate related work are been done when the person whom the certificate need to issued is physically present in front of officers.

A. Problem Statement

Our system mainly consist of key logger, shuffle keypad & QR Code which provide security at the time of login and Information transfer. Before person can login, he/she needs to get registered in system by filling the registration form. Then login process includes sending the otp on mail box, after successfully entering the otp, shuffle keypad gets enable so that password can be entered. Once the login is success, user has the option to apply for various document/certificate by filling the request forms. The request submitted by user goes to general authority of State Government/Union Territory. Authority login can view the requested information in the from of QR Code, so we have developed the android application to decrypt information. And based on that authority can approve the request or else deny it. Once the request is approved, user get the required certificate in his account, so that user can download it. ALGORITHM } AES Algorithm } The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data?the data to be encrypted. This array we call the state array. } You take the following aes steps of encryption for a 128-bit block Derive the set of round keys from the cipher key. } Initialize the state array with the block data (plaintext). Add the initial round key to the starting state array. } Perform nine rounds of state manipulation. } Perform the tenth and final round of state manipulation. } The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others. }

Note: AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds..

II.   LITERATURE SURVEY

A literature review is a text of a scholarly paper, which includes the current knowledge including substantive findings, as well as theoretical and methodological contributions to a particular topic. Literature reviews use secondary sources, and do not report new or original experimental work.

1. Paper Name: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes Author: Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajanoy. 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, deploy ability and security benefits that an ideal scheme might provide.

2. Paper Name: Safe Slinger: Easy-to-Use and Secure Public-Key Exchange Author Name: M Farb, Yue-Hsun Lin, Tiffany Hyun-Jin Kim, Jonathan McCune, A Perrig 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.

3. Paper name: Leveraging Personal Devices for Stronger Password Authentication. Author Name: Mohammad Mannan and P.C. Van Oorschot Internet authentication for popular end-user transactions, such as online banking and ecommerce, continues to be dominated by passwords entered through enduser PCs.

4. Paper name: Designing Leakage Resilient Password Entry on Touchscreen Mobile Devices. Author name: Qiang Yany, Jin Hanz, Yingjiu Liy, Jianying Zhouz, Robert H. Dengy. 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.

5. Paper name:- GANGS: Gather, Authenticate 'n Group Securely. Author name: Chia-Hsin Chen, Chung-Wei Chen, Cynthia Kuo, Yan-Hao Lai, Jonathan M. McCune, Ahren Studer, Adrian Perrig, Bo-Yin Yang, Tzong Chen Wu. Mobile users share the same expectations as wired users: they want to communicate with other people, they expect the communication to be secure, and it should all be easy.

III. ARCHITECTURE
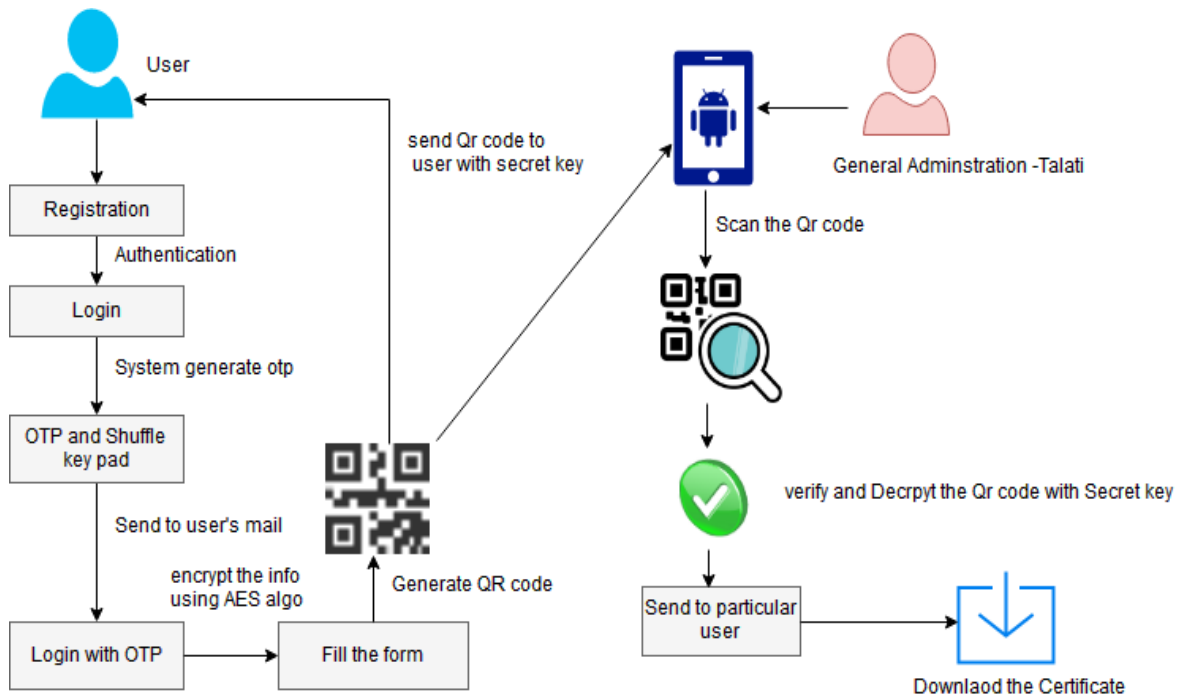
IV. METHODOLOGY

1. We are using waterfall model for our project. Requirement gathering and analysis: In this step of waterfall we identify what are various requirements are need for our project such are software and hardware required, database, and interfaces.

2. System Design: In this system design phase we design the system which is easily understood for end user i.e. user friendly. We design some UML diagrams and data flow diagram to understand the system flow and system module and sequence of execution.

3. Implementation: In implementation phase of our project we have implemented various module required of successfully getting expected outcome at the different module levels. With inputs from system design, the system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing.

4. Testing: The different test cases are performed to test whether the project module are giving expected outcome in assumed time. All the units In spite of his busy schedule he devoted himself and took keen and personal interest in giving me constant encouragement and timely suggestion. It gives me a great pleasure in presenting the report of my project. I take opportunity to express my deep sense of gratitude to our Principal Dr. Mukane who helps us. I would be failing our duty if I do not thank our HOD Prof. Shah for his word of encouragement and special guidance and vital inspiration. With deep reverences!!!!

V.   CONCLUSION

We are currently in the process of developing a project titled "EDOCUMENTS WITH APPLIED QRCODE AND KEYLOGGING SECURITY." This project aims to provide a highly secure environment, safeguarding against external threats such as hackers and shoulder surfing. It will empower users to remotely apply for any certificate, irrespective of their location.

ACKNOWLEDGEMENT

VI.   REFERENCES

[1]   World. Health. Organisation. The top ten causes of death. [Online].Available: http://www.who.int/mediacentre/factsheets/fs310/en/

[2]   C. Saiprasert and W. Pattara-Atikom, "Smartphone enabled danger- ous driving report system," in Proc. HICSS, 2013, pp. 1231–1237.

[3]   M. V. Yeo, X. Li, K. Shen, and E. P. Wilder-Smith, "Can svm be used for automatic eeg detection of drowsiness during car driving?" Elsevier Safety Science vol. 47, pp. 115–124, 2009.

[4]   S. Al-Sultan, A. H.Al-Bayatti, and H. Zedan, "Context-aware driver behavior detection system in intelligent transportaion system," IEEE Trans. on Vehicular Technology, vol. 62, pp. 4264–4275, 2013.

[5]   J. Paefgen, F. Kehr, Y. Zhai, and F. Michahelles, "Driving behavior analysis with smartphones: insights from a controlled field study." 2012.

[6]   Y. Wang, J. Yang, H. Liu, Y. Chen, M. Gruteser, and R. P. Martin, "Sensing vehicle dynamics for determining driver phone use," in Proc. ACM MobiSys, 2013.

[7]   H. Han, J. Yu, H. Zhu, Y. Chen, J. Yang, Y. Zhu, G. Xue, and M. Li, "Sen speed: Sensing driving conditions to estimate vehicle speed in urban environments," inProc. IEEE INFOCOM, 2014.

[8]   S. Reddy, M. Mun, J. Burke, D. Estrin, M. Hansen, and M. Srivastava, "Using mobile phones to determine transportation modes," ACM Trans. on Sensor Networks vol. 6, no. 13, 2010.