Applied GIS

ISSN: 1832-5505

Vol-4 Issue-02 APRIL 2016

Security for Electronic Documents using Keylogging and QR Codes

Dhanashree Gujar[#1], Vrushali Mane[*2], Abhishek Pandey[#3], Shubham Dhumal[*4], Prof.Shwetkranti Taware[#5]

[#]*Computer Department, Indira College of Engineering and Management,Savitribai Phule University,Pune,India*

Abstract— *In this digital era of computer and technology, we are still lacking behind when it comes to government offices documentation work and processes. In order to get nay work done which involves our national government, there is a long procedure and unnecessary queues. Moreover, its harsh reality that government official takes more than instructed time to accomplish any work related to public. It's difficult for senior citizens to be present every time and wait in long queue Worst case scenario is that sometimes after submitting al the required documents, they inform us that they have misplaced or not received any one of the document. In this case even though we have submitted we do not have any option rather than resubmitting again so that our process is completed. This is too tedious and time consuming. Thus to avoid all this document loss and steady up the current procedure we have come up with a digital solution that guarantees reliability, no document loss and safety along with fast processing and thus not only helping working citizens but also senior citizens from standing in long queue.*

Keywords— **E-Documentation, QR Code, Digital processing, Encryption, Cryptography, Government key logger.**

INTRODUCTION

Despite the perception that today's communication is conducted almost entirely through electronic media, many messages continue to be produced in a word-processing program rather than directly as emails, texts, and tweets, and are transmitted through various postal services. Communicating in hard copy through the postal service continues to be necessary because of a variety of factors, including a lack of access to electronic media by a percentage of the population, as well as failure by some of those who have access to use it to access the internet for information. Privacy regulations have also made it difficult for those sending information to a general population to access email addresses or mobile-phone numbers for texts. Electronic documents, or eDocuments, are paperless account documents available in PDF format (Adobe Acrobat required). You can view, save or print your eDocuments at your convenience, and will remain in the online site archive for seven years, provided the account remains open. Once an account is closed, you cannot access e-Documents associated with that account.

We have come in digital era where everything is being digitized from email, messages, payments and everything is just a click way. But in this digital era also when it comes to government process we still have the old mundane tedious process of standing in queue and getting our work done. Also its harsh reality that most of the time we have to pay bribes to get things done faster. Thus there is no transparency and no methodology which can be followed. Currently to acquire any government document we need to follow old lengthy procedure which is time and energy consuming. Hence to overcome these issues we are proposing an E-Documentation system using QR code and provide AES security.QR codes have emerged as a popular medium to make content instantly accessible. With their high information density and robust error correction, they have found their way to the mobile ecosystem. However, QR codes have also proven to be an efficient attack vector, e.g. To perform phishing attacks. Attackers distribute malicious codes under false pretences in busy places or paste malicious QR codes over already existing ones on billboards. Ultimately, people depend on reader software to ascertain if a given QR code is benign or malicious.

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches. However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

This proposed system not only saves time but money and resource and guarantees a secure transmission of documents online. These can be easily shared, can have a transactional log file in case lost and can be easily recoverable unlike the current scenario.Also the original documents can be always safeguarded and need not to be used once while waiting for other procedure to be completed. Our proposed system cover all the drawbacks of current system and provides a solution which is more secure, reliable and time saving.

PROBLEM STATEMENT

With the rapid development of the cloud computing, online document record has attracted great attention of many researchers all over the world recently. However, E-documents, which has many security and efficiency issues. Therefore, the study of secure and efficient E-documents Record Scheme to protect users' privacy in E-documents files is of great significance. Focusing on drawbacks and inadequacies of existing process, definitely there is a need of an efficient system which ensures datasecurity.

LITERATURE SURVEY

1) **SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud Author: Mazhar Ali, Assad Abbas,Muhammad Usman,Shahid Khan and Samee U. Khan**

The widespread acceptance of cloud based services in the healthcare sector has resulted in cost effective and convenient exchange of Personal Health Records (PHRs) among several participating entities of the e-Health systems . Nevertheless, storing the confidential health information to cloud servers is susceptible to revelation or theft and calls for the development of methodologies that ensure the privacy of the PHRs. Therefore, we propose a methodology called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the confidentiality of thePHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi-trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re-encryption keys. Moreover, the methodology is secure against insider threats and also enforces a forward and backward access control. Furthermore, we formally analyze and verify the working of SeSPHR methodology through the High Level Petri Nets (HLPN). Performance evaluation regarding time consumption indicates that the SeSPHR methodology has potential to be employed for securely sharing the PHRs in the cloud.

2) **The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes (2012) 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 us-ability, 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 authen-tication 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. This paper 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 bench-mark for future web authentication proposals.

3) **SafeSlinger: Easy-to-Use and Secure Public-Key Exchange (2011) Author: 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 help-lessness ofusers. To establish a secure basis for online communication, we propose SafeSlinger, a system leveraging the proliferation of smartphones to enable people to securely and privately exchange their public keys. Through the exchanged authentic public keys, SafeSlinger establishes a secure channel offering secrecy and authen-ticity, which we use to support secure messaging and file exchange. SafeSlinger also provides an API for importing applications public keys into a users contact informa-tion. By slinging entire contact entries to others, Paper propose secure introductions, as the contact entry includes the SafeSlinger public keys as well as other public keys that were imported.

4) **Leveraging Personal Devices for Stronger Password Authentication (2011). Author:Mohammad Mannan and P.C. van Oorschot**

Internet authentication for popular end-user transactions, such as online banking and e-commerce, continues to be dominated bypasswords 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 keylogging, phishing, and pharming.The paper propose Mobile Pass- word Authentication (MP-Auth) to counter such attacks, which cryptographically separates a users 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 users 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 recipients public key. MP-Auth expects user to input passwords only to a personal device, and be vigilant while confirming additional trans-actions from the device. To

facilitate a comparison to MP-Auth, In this paper also provide a comprehensive survey of web authentication techniques that use an factor of authentication; this survey may be of independent interest.

5) **GAnGS: Gather, Authenticate n Group Securely. Author: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. However, mobility poses many challenges for security. Communication is often ad hoc, and the infrastructure may be untrusted. Secure communication relies on the distribution of authentic information among the communicating parties devices. This is a challenging problem because devices generally do not share preexisting secrets. Current security protocols for distributing initial authentic information fail to consider the human element. Many protocols do not scale beyond a pair of devices, although people often need to communicate with a group. The few existing group protocols assume that users will always count the number of members and verify the list of members correctly. However, as group size increases, implementations of these protocols become more prone to human error. Paper present GAnGS, a fully-implemented system for exchanging authentic information between mobile devices when they are physically present in the same location. GAnGS is scalable, appropriate for two or more devices. Paper implement two user friendly variants of GAnGS on Nokia N70 camera phones. The first variant, GAnGSP, is based on an untrusted communication hub. Thesecond variant, GAnGS-T, needs no infrastruc-ture. Both variants use Bluetooth for peer-to-peer wireless communication during the information exchange.

6) **Efficient Implementation of the AES Algorithm for Security Applications.Author: Shady Mohamed Soliman*, Baher Magdy*and Mohamed A. Abd El Ghany** Electronics Department, German University in Cairo, Cairo, Egypt***

In this paper, area, throughput and power optimized designs for AES-128 bit algorithm are introduced. AES-128 bit is composed of 10 rounds with a key expansion module that generates 10 keys for the 10 rounds. These keys are either generated , saved and used later for the 10 rounds [10-13] or they are computed on the fly for each round [14] and [15] The proposed designs reduce area and power by exploiting the iterative looping idea as well as the key expansion module which computes the keys on the fly. They also makes use of pipelining through multistage pipelined registers to achieve best throughput possible. Moreover, this optimization makes these designs compatible with latest security applications, especially those embedded in low power modules such as: Xbee and Bluetooth low energy (BLE) which are the main enabling technologies for internet of things (IoT) applications.

SYSTEM ARCHITECTURE

In our proposed system, we are building a secure, encrypted and complimented with QR code an E-Documentation system. Thisis more secure and reliable and deprived of any external attacks. Here we would be having an user portal and a web portal along with an android application to scan the QR code. The basic functionality of this system is that whenever an user want to get any government document created or services which require to submit government documents; he needs to first register and login to the system. Here login functionality is completed using an OTP which user will receive and later needs to change as per their convenience. Once successfully logged in, there an option for uploading the required documents. Each document has a unique document ID or number, for example adhar card has 12 digit adhar number. All these documents would be encrypted using encryption algorithm. But as we know there are slight chances of attacks and data can be easily decrypted hence we have added a more secure QR code functionality. All these documents and encrypted documents will be hidden behind a QR code. Third party such as government officials will have a unique R code scanner through which they can decrypt the data behind QR code and thus proceed with the process. This system maintains transparency, security and reliability and is more time and energy saving.

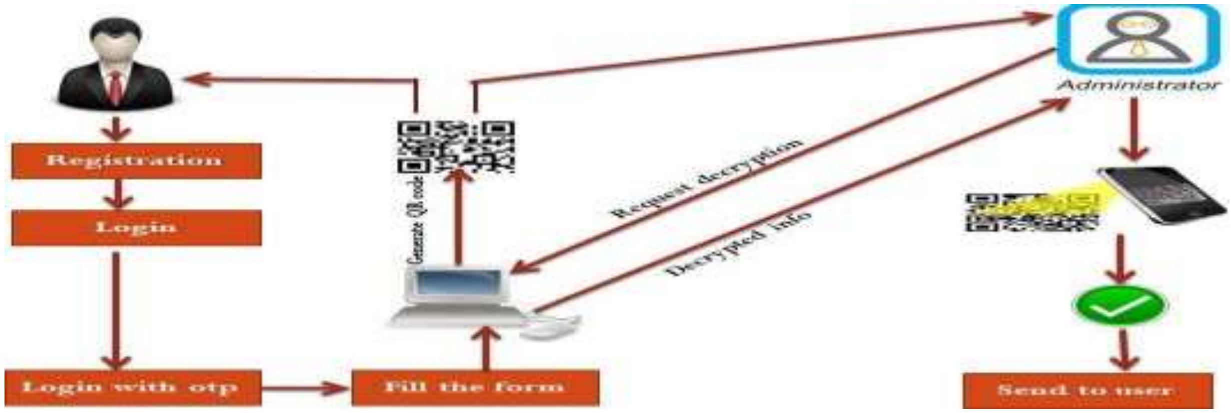

Fig. 1 System Architecture

ALGORITHM

A. *AES Aglorithm*

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher that comprises three block ciphers, AES- 128, AES-192 and AES-256[9]. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively [3]. Based on the key length used, the number of execution rounds of the algorithm is 10, 12 or 14 respectively. The proposed design is based on the AES-128 Encryption. Each 128-data bits block along with the 128-bit cipher key are processed through a 4 x 4 state matrix and key matrix respectively. At the start of the algorithm, the state matrix is initialized with the original plain text while the key matrix is initialized with the user input key. Fig.1shows the AES-128 encryption steps that consists of 10 rounds. Through each round, Each of the two matrices proceeds in different paths undergoing different procedures and their outputs are combined at the end of each round in the AddRoundKey phase. The round block that processes the state matrix consists of four main transformations: SubBytes, ShiftRows, MixColumns and AddRoundKey. The algorithm starts by executing the AddRoundKey transformation on the original plain text and cipher key. Moreover, the last round of the algorithm differs from the previous 9 rounds as it excludes the Mix Columns transformation. On the other hand, the cipher key undergoes different processing steps as it is subjected to a Key-Schedule operation where it expands into 10 keys throughout the 10 rounds of the algorithm. Each step is explained in the following sub-sections.

1) *SubBytes Transformation*

A non-linear substitution for each byte in the state matrix with a corresponding byte value based on a lookup table called S- box (Substitution Box). Each value in this table is calculated by determining the multiplicative inverse over GF(2 8) followed by an affine transformation.

2) *ShiftRows Transformation*

Each row of the state matrix has its bytes cyclically shifted to the left by a certain offset, Where Row n is cyclically shifted to the left by n - 1 bytes. This means that the first row is left unchanged.

3) MixColumns Transformation

A transformation in which each 4 - byte column of the state matrix is considered as a four-term polynomial over GF (2 8) and multiplied modulo x 4 + 1 with a fixed polynomial a(x), where: a(x) = {03}x3 + {01}x2 + {0l}x + {02}

3) AddRound Key Transformation

A simple bitwise XOR operation between each byte in the state matrix with its corresponding byte in the key matrix. The keymatrix corresponds to the same round of the state matrix.

4) KeyExpansion

This phase generates 10 different expanded keys from the original key cipher to be used respectively in each round of the AES algorithm. Each column in the new key is generated from its preceding expanded round key column as described by (2) and (3).

Wr,i = Wr-1,i XOR Wr,i-1, 0 < i <4,(2)

Wr,0=SubWord(RotWord(Wr-1,3))XOR Rcon[r] XOR Wr,0,(3)

The notation Wr,i refers to the 4-byte column number i in the round number r, Where r is from 0 to 10. The function SubWord in (3) applies the SubBytes transformation on each of the 4 bytes of the given word. The function RotWord performs a left cyclic shift by 1 byte on the given word. Furthermore, the Rcon[r] is the 32-bit word given by [x r-1 , {00}, {00}, {00}]

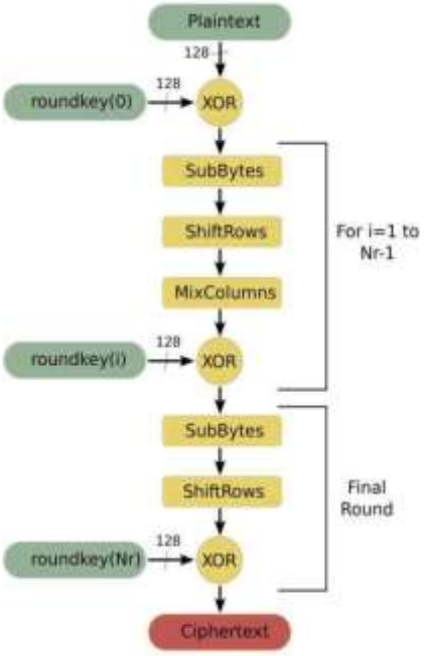

Fig. 2.Advance Encryption Standard

B. *QR-CODE*

The foursquare Quick Recognition (QR) code consists of coding region and functional regions. The coding region is described by some characters, which represent the data, version, format, and so on. The functional regions are the combination of localization graph, correcting graph, separator and some seeking graphs, which would not be used for data encoding. The region of four module wide around the QR code image is named as blank, which has the same reflective index with light-colored modules. The most remarkable regions are three graph blocks used for image seeking. The three graph blocks locate at the top left comer, left lower comer and the top right comer of the QR code image, respectively.

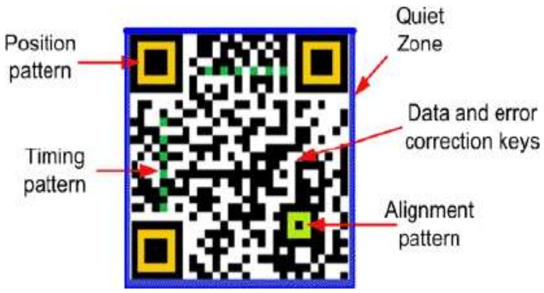

Fig. 3. QR-Code

IMPLEMENTATION.

In the proposed system, E-documents information of the user will be stored in a form of data will be stored in an encrypted format for security purposes. Advance Encryption Standard (AES) will be used for the process of encryption. This encrypted data will be saved on secured cloud. A QR code will be generated .To extract the data from the cloud the Adminstrator will be required to scan the QR code to access the data. After authentication the decrypted data will be displayed to the authenticated user.The module shown below will give a clear idea of our proposed system.

I. Login

When users access the system through Portal Direct Entry, they are considered guests until they log in. The Login Module is a portal module that allows users to type a user name and password to log in.The module is no longer available to users after theyhave logged in.

II. Fill the form

User need to select which document he wants to issue and then fill the form for that.Form will contain all the information ofuser required to issue the documents.

III. Encrption and QR-CODE

After the user fills the form all the information submitted by the user will be encrypted using AES algorithm.Once the data isencyprted QR code will be generated for the information.This QR-Code will be received by government officials.

IV. Decrpytion and scanning

Once the officials receives the QR-code they will scan this QR-code using scannerand then the data will be decrypted and allinformation will be verified by government officials.

V. Download documents

When all the data will be verified users e-document will be generated by officials.This certificate will be send to user so thatuser and download certificate by logging into his account.

CONCL USIONS

In this work, we have proposed digital, hassle free, time saving system for documentation system. Our proposed system not only provides security but also has unique QR code scanner which can only be used by authorized personnel only.

This system maintains transparency and keeps record of each and every transaction. Third party will have a portal which they can log in using user id and password. All the documents which user has sent for processing can be decrypted using QR code scanner only. All the data would be verified and kept in database for processing and future reference. Thus there would be no document loss and a user need not to be physically present and wait in long queues. This system is more user friendly, easy, convenient and secure and also reduces manual effort to great extent

ACKNOWLEDGMENT

With all respect and gratitude, we would like to thank all the people who have helped us directly or indirectly for the completion of the project “Secure sharing of E-documents using QR-code and Key logging Security”.

We express our heartily gratitude towards Prof.Shwetkranti for guiding us to understand the work conceptually and also for her constant encouragement to complete the project. Our association with her as a student has been extremely inspiring. We would like to give our sincere thanks to Dr.Poorna Shankar , Head of the Department of Computer Engineering for her technical support and constant encouragement. We would also like to extend our sincere thanks to our Principal Dr.Sunil Admuthe for his help and support in all respects. We would also like to thank all our staff members and colleagues who helped us directly or indirectly throughout our dissertation work.

REFERENCES

[1] C. Yue and H. Wang, BogusBiter: A transparent data encryption system against phishing attacks, ACM Trans. Int. Technol.,vol. 10, no. 2, pp. 131, May 2010.

[2] Q. Chen, S. Abdelwahed, and A. Erradi, A model-based approach to self-protection in computing system, in Proc. ACM Cloud Autonomic Comput. Conf., Miami, FL,USA, 2013, pp. 110.

[3] H. Lu, B. Zhao, X.Wang, and J. Su, DifiSig: Resource dier- entiation based malware behavioral concise signature generation, Inf. Commun. Technol., vol. 7804,pp. 271284, 2013.

[4] Z. Shan, X.Wang, T. Chiueh, and X. Meng, Safe side eects commit- ment for OS-level virtualization, in Proc. ACM Int. Conf. Autonomic Comput., Karlsruhe,Germany, 2011, pp. 111120.

[5] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, Detecting web based DDoS attack using MapReduce operations in cloud computing environ- ment, J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 2837, Nov. 2013.

[6] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, MIS: Malicious nodes identification scheme in network-coding-based peer- to-peer stream- ing, in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 15.