International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

AUTHENDICATION PERMISSION GRANTING ALGORITHM FOR TRANSACTION OF SENSITIVE INFORMATION USING QR CODE

J. Sharon Chella Priyanga[1], A.S Balaji[2]

[1]PG Student, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology, Tamil Nadu, India.
[2]Assistant Professor, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology, Tamil Nadu, India.

Abstract - *A remote data integrity document is highly confidential data stored in the cloud. Encrypting the whole shared file can discern the confidential information hiding, but still this shared set of file will be unable to be accessed by third party. A remote document reference id automatically converts to the QR code can be scanned by the entity module. The access to the shared remote data integrity is permitted to download the particular document integrity that realizes data sharing with sensitive information hiding. Implementing RFID techniques can emerge a problem, where the liquid and metal surfaces tend to reflect radio waves. When this RFID reader reads the information in case the tags are installed in liquid or metal products becomes tedious process. Introducing QR-code generate algorithm documents can be remotely stored in the cloud and realize the data sharing with other entities which also contains some sensitive data. QR code proves to be too expensive for many applications as compared to other tracking and identification methods, such as the simple barcode. The sensitive information should not be exposed to third party entities when the cloud file is shared. Signatures are used to verify the file in the phase of integrity to realize data sharing with sensitive information hiding in remote data integrity.*

Key Words: Cloud storage; Data sharing; Data integrity auditing; confidential information hiding.

1. INTRODUCTION

Nowadays context-aware applications have multiply with the increasing popularity of smart phones and are prepare with a different sensor types namely GPS, light, microphone, accelerometers, and proximity sensors. These sensors could sense the surroundings and the status regarding to a Smartphone, and the sensed data can be used to infer the present context or the behavior of the user. For example, GPS data can provide information about location

By using the contexts, an increasing number of applications on smart phones are designed and developed to provide personalized context aware services.

Examples of such context-aware applications L. Zhang and X. Wang are with the Ministry of Education Key Laboratory for Modern Teaching Technology, Xi'an 710062, China, and with the School of Computer Science, Shaanxi Normal University, Xi'an 710119, and China. Z. Cai is with the Department of Data mining is the procedure of finding patterns in large data sets that implicate the intersecting the concept of database systems and statistics, machine learning. In addition for field like businesses, data mining is used to learn and understand the patterns and relationships in the data in order to proceed by uttering better business decisions.

A cloud refers to an environment that is designed for the purpose of remotely provisioning scalable and measured IT resources. Where the network providing remote access to a set of decentralized IT resources.

The idea behind the project is to design an mobile application for Data Sharing through cloud storage service, users can remotely store their data to the cloud and realize the data sharing with other entities which also contains some sensitive data.

The sensitive information should ensure it is retrieved by the authenticated user when the cloud file is shared. In this scheme, a sanitizer is used to sanitize the information corresponding to file and transforms these information's signatures into valid ones for the sanitized file.

These signatures are used to check the rectitude of the sanitized file in the phase of integrity auditing. In data sharing between two entities in cloud one part hospital management to treat as the admin part and then patient to treated as the user part. Admin to upload the medical record in our cloud (Data and patient ID) then search the particular patient id and medical document reference id automatically convert to the QR code then just scan user module then download the particular document.

The main advantage is to have more secured transition between two sides, more flexible, easy-access; finally we can download the document as a free report. In existing system they have used RFID technology which is not suitable for more sensible data storing and not compact for all sectors.

There are many organizations and individuals who might like to store their data in the cloud. However, the data stored in the cloud might be corrupted or lost due to the inevitable software bugs, hardware faults and human errors in the cloud Providing Security for the medical document using QR

code base Android application. Where User can store their documents in cloud

Which will be converted into QR code which can be downloaded by the particular person who have gained the access to the document and they can share it with the corresponding entities. This brings the trust worthy among the users to upload their catalogue in cloud where admin uploads the document along the reference id which then automatically generates the QR code.

A remote data integrity document is suggested to assurance the integrity of the highly confidential data stored in the cloud. Encrypting the whole shared file can discern the confidential information hiding, but still this shared set of file will be unable to be used by any other third party.

User can store their documents in cloud which will be converted into QR code which can be downloaded by the particular person who have the access to document and they can share it with the person whom they are willing to.

In order to verify whether the data is stored correctly in the cloud, many remote data integrity checking schemes have been proposed.

In remote data integrity auditing schemes, the data owner firstly needs to generate signatures for data blocks before up-loading them to the cloud. These shared data stored in the cloud might contains some sensitive information of the patient such as patient's name, telephone number and ID number, etc. and it might also contain some hospital's Sensitive information relating to hospital details such as hospital's name, etc.. Hence patient and hospital details will be inevitably exposed to the cloud and the researchers. Hence, it is necessary to accomplish remote data integrity on the condition that the sensitive information of shared data is protected.

To solve this problem efficiently, we can initially, encrypt the whole shared document before transferring it to the cloud, secondly generate the signature that is used to check the integrity of this encrypted file, and then upload the encrypted file with its corresponding signatures to the cloud. Using this method the sensitive information hiding can be decrypted by the owner of the document. Hence it prevents unauthorized access.

The result that we try to attain is, it is impractical to hide sensitive information by encrypting the whole shared document.

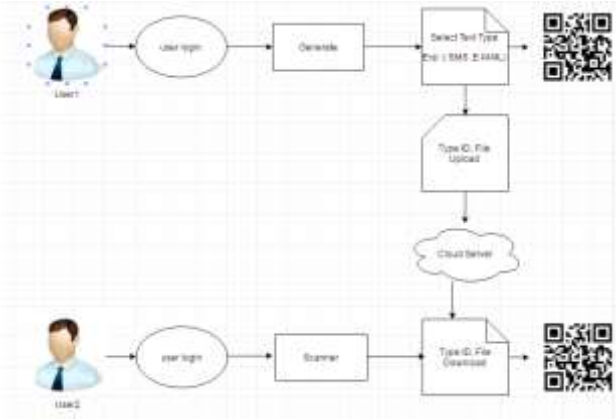

Figure 1.1

PROBLEM STATEMENT

Remote data integrity documents are suggested to assurance the integrity of the highly confidential data stored in the cloud. Encrypting the whole shared file can discern the confidential information hiding, but still this shared set of file will be unable to be used by the other enties. We introduce a remote document reference id automatically convert to the QR code then just scan user module. Were access is permitted to download the particular document integrity that realizes data sharing with sensitive information hiding. Signatures are used to verify the file in the phase of integrity auditing.

1.1 OBJECTIVE

User can store their documents in cloud generating a QR-code where the document will be hidden in this QR-code that can be downloaded by the particular person who have the authenticated key to access the document.

1.2 SCOPE

- Easily send the auditing documents in QR code.
- Medical field, where the patients documents can be viewed by the particular concern doctors.
- private message sharing and document authentication using QR code
- Auditing field, where the business deals can be maintained with high security.
- Army, navy, air force, the country is our pride where there is a necessary to maintain the highly confidential document with high privacy.
- In addition this idea can also be used in the research filed preventing from unauthorized access.

2. OPEN HANDSET ALLIANCE

The open handset alliance (OHA) is a business alliance to develop open standard. By developing this technologies

will lower the cost of developing the mobile devices and services.

ANDROID ARCHITECTURE

The software stack is split into Four Layers:

1. The application layer
2. The application framework
3. The libraries and runtime
4. The kernel

1. THE APPLICATION LAYER

This application layer is the upper layer in android architecture. The applications features like Google map, browsers, scanners, SMS messaging tools browsers, phone contacts, navigation applications and calendars works with end users with the help of application framework to operate.

2. APPLICATION FRAMEWORK

In application frame work the classes and services are mandatory for developing the application. Where the developers are given access to reuse and extend their components which is already present in API. Managers are enabled in this application for accessing the data.

(i) ACTIVITY MANAGER:

The lifecycle of the application is managed by this activity manager. Enabling the proper management for all activities. Meanwhile this activity is controlled by the activity manager.

(ii) RESOURCE MANAGER:

Resource manager enables the access to non-code resources like graphics etc.

(iii) NOTIFICATION MANAGER:

It activates all application's to be display under the custom alerts in status bar.

(iv) LOCATION MANAGER:

It triggers alerts immediately user enters or leaves a specified geographical location.

(v) PACKAGE MANAGER:

It is used to retrieve the data that is about to installed packages on a particular device.

(vi) ACTIVITY MANAGER:

The lifecycle of the application is managed by this activity manager. Enabling the proper management for all activities. Meanwhile this activity is controlled by the activity manager.

(vii) WINDOW MANAGER:

It creates views and layouts. Used to create the user interface modules.

(viii) TELEPHONY MANAGER:

It is used to handle setting the information about all the services device and for setting the network connection

(ix) ANDROID RUNTIME:

The android applications are executed in this section. Because android has its own virtual machine

I.e. DVM (Dalvik Virtual Machine), which is designed and used for execution of the android application. Where users are given access to execute multiple applications at the same time.

3. LIBRARIES:

Android provide their own libraries which is written using C/C++. These libraries are not given access to enable directly. Hence application framework is used to enable the access, they are provided with many libraries such as access web browsers, libraries and, video format.

4. LINUX KERNEL:

This layer is the main layer for android architecture because it provides service like memory management, security, power management. This layer is used for better binding for hardware and software to provide good communication between them.

3. SECURITY

Android is a multi-process system, in which each application is executed in its own process. The most of the securities between applications and the system is enforced at the process level through standard Linux

facilities, such as user and group IDs that are assigned to applications.

Android provides flexibility because it was designed with the multilayer architecture hence it provides the security from the attackers.

4. LIMITATIONS OF ANDROID:

Development requirements in
Java Android SDK Eclipse IDE (optional)

5. DISADVANTAGES

However, the current state of employing digital humanities in teaching most innovative developments that have taken the Internet from passive desktop publishing to 'social media' or from text to 3D immersive virtual realities.

Encrypting the shared file will realize the sensitive information hiding, which cannot be used by others. Less security hence, not trustable.

6. PROPOSED SYSTEM:

We propose a remote data integrity that realizes data sharing with sensitive information hiding using QR code.

We hide the highly confidential document using the QR code.

In data sharing between two entities in cloud one part hospital management to treat as the admin part and then patient to treated as the user part. Admin to upload the medical record in cloud (Data and patient ID) then search the particular patient id and medical document reference id automatically convert to the QR code then just scan user module then download the particular document. The main advantage is to have more secured transition between two sides, more flexible, easy-access; finally we can download the Document as a free report. A sanitizer is used to sanitize the data blocks containing any sensitive information of the file and transforms these data blocks' signatures into valid ones for the sanitized file.

These signatures are used to verify the integrity of the sanitized file in the phase of integrity of QR code generate Algorithm.

QR code proves to be too expensive for many applications as compared to other tracking and identification methods, such as the simple barcode.

FEATURES OF QR-CODE:

High data encoding capacity:

The maximum QR code symbol can encode about 7089 characters.

High-speed scanning and reading:

QR code reader can recognize as many as QR code symbols this helps them to read the data fast.

Capable of reading Japanese and Chinese encoding:

QR codes can also read Japanese and Chinese characters as fast as English characters. Because the QR code system was invented by the Japanese company during the year 1994 for the purpose of tracking vehicles along with it, it was also designed with the high speed component scanning.

Can be read from any direction:

It is a matrix of 2D code, and it is possible to scan and read the data from any direction.

7. MODULES

1. Registration
2. QR Code Generator
3. File Hiding
   (a) The Correctness
   (b) Sensitive Information Hiding
   (c) Correctness Soundness
4. QR Code Scanner
5. File Sharing
6. Request for Permission
   (a) Setup
7. Permission Generation
   (b) Extract
   (c) SigGen

1. REGISTRATION:

The modules describe signup page contains email id or user name, password and conform password those kind of details form the client should be stored in database.

Login screen contains email id or username and password when the user to login the app it should retrieve the data from the database and combine based on user input if its match user name and password to allow in the user to login otherwise alert and show a message to the user.

2. QR CODE GENERATOR:

This module Used to Generate the QR- code for the User enters Key and additionally what kind of data likes text, image, etc.

3. FILE HIDING:

(a) The Correctness
(b) Sensitive Information Hiding
(c) Correctness Soundness

(a) THE CORRECTNESS:

- The correctness has the three necessary procedures which is followed one after the other systematically
- Checking for the Private Key correctness
- The correctness of the blinded file and for its corresponding signatures

(b) SENSITIVE INFORMATION HIDING:

- The user ID of a patient takes the input as the original file F along with the user's private key Skid and outputs the blinded file F

(c) CORRECTNESS SOUNDNESS:

To assure that if the cloud does not truly store user's intact sanitized data, it cannot pass the TPA's verification.

4. QR CODE SCANNER:

In, Additionally One type of application name as (QR-droid) used in this project. QR-droid is used to scan the any kind of User QR-code. Initially, User1 generate the QR-code after that QR-code is sent to the User 2. Then User2 Scan the QR-code and get the key.

5. FILE SHARING

(a) File uploading:

In this Module used to upload the document, the user 1 knowing the key, and what kind of data to be upload from gallery to Server. Finally the data and key to uploaded to the Server.

(b) File downloading:

In this Module Explain that, After Getting the Key from User 2 then Enter the key in Download Process and Get the File from Server.

6. REQUEST FOR PERMISSION:

In this request for permission Phase the PKG i.e. (Primary key Generation) is generated by the client. This PKG is trusted by other entities. It is responsible for generating system public parameters and the private key for the user according to his identity ID. This PKG run the setup algorithm. It takes input as a security parameter (k). Then outputs the master secret key MSK and the system public parameters pp.

The user say for example, from the client side must request for the patient report, this request is sent to the admin portal, once this admin portal is viewed by the admin and the access is permitted to the client, then patient report hidden in the QR code is generated in the patient portal. Now the patient can scan the QR code and allowed to download the patient report.

STEP 1: Setup algorithm run by the PKG. It takes as input a security parameter k. It outputs the master secret key MSK and the system public parameters pp.

7. PERMISSION GENERATION:

The admin will grant the TPA (Third Party Authentication) which is the public verifier. It is in-charge of verifying the integrity of the data stored in the cloud on behalf of users.

PKG runs the extraction algorithm, where It takes the system public parameters pp, the master secret key MSK and the user's identity ID as input, and outputs the user's private key SKID.

The user can verify the correctness of SKID, only if it passes the verification, then the QR code is generated in the client's portal; if the correctness is mismatched then the QR code will not be generated in the client's portal.

STEP 2: PKG perform extraction Taking input as, system public parameters pp, the master secret key msk, and a user's identity ID. It outputs the user's private key skID. The user can verify the correctness of skID and accept it as his private key only if it passes the verification.

STEP 3: For each user ID requested for the patient report assigns input as, the original file F, the user's private key SKID, the user's signing private key ssk and the file identifier name. And outputs a blinded file F*, along with its corresponding signature set Φ.

8. ALGORITHM

(a) MERKLE HASH TREES ALGORITHM:

The aim of the algorithm is to verify the integrity of the data stored in the cloud. The x hold elements in Z*p and G1 hold the elements such as μ0, μ1, μ2..., μn, g2 from a public value. The data stored in the cloud can be retrieved and the integrity of these data can be ensured based on pseudo random function and BLS signature.
The data integrity of the cloud is verified by the following:

One large prime p contains Multiplicative cyclic groups with order p

The Multiplicative cyclic groups G1, G2 are mapped by bilinear pairing map

e: G2 F(X) ⟵ G1 × G1

The original file F, such as F = {m1, m2, ..., mn} is blinded by the cryptographic hash function: G1 ⟵ H : {0, 1}*

The key is generated for the set of indexes of the data blocks corresponding to the personal sensitive information is indicated as K1

Φ = {σi}1≤i≤n the signature is generated for the set of the blinded file F*

The msk (master secret key) and skID (private key of the user ID) is generated in hash function G1 ⟵ H : {0, 1}*

The F* = {m*1, m*2, ..., m*n} the blinded file F* is ready to be sent to the sanitizer

Φ 0 = {σ 0 i}1≤i≤n the signature is generated for the set of the sanitized file F0

Then the key is generated for the set of the indexes of the data blocks corresponding to the organization's sensitive information

Finally, F0 = {m01, mo2, ..., m0n} the sanitized file F0 stored in the cloud

(b) AUTHENDICATION PERMISSION GRANTING ALGORITHM:

STEP 1: Setup algorithm run by the PKG. It takes as input a security parameter k. It outputs the master secret key MSK and the system public parameters pp.

STEP 2: PKG perform extraction Taking input as, system public parameters pp, the master secret key msk, and a user's identity ID. It outputs the user's private key skID. The user can verify the correctness of skID and accept it as his private key only if it passes the verification.

STEP 3: For each user ID requested for the patient report assigns input as, the original file F, the user's private key SKID, the user's signing private key ssk and the file identifier name. And outputs a blinded file F*, along with its corresponding signature set Φ.

9. FUTURE ENHANCEMENT

In future it will have more feature like Online chat, video calling and these are used to get the details within the minute. We are going to develop an Advance learning system, which adopts the designed scheme to trace visitors' trajectories in our campus. Besides, we are now going to apply the designed scheme to analyze sport postures.

TECHNIQUE DEFINITION:

Human Segmentation Algorithm where the Human region segmentation algorithm for real-time video-call applications. Unlike conventional methods, the segmentation process is automatically initialized and the motion of cameras is not restricted. To be precise, our method is initialized by face detection results and human/background regions are modelled with spatial color Gaussian mixture models (SCGMMs).

EXTR ADVANTAGES:

- User friendly
- It will take less time to transfer huge volume of data.
- Efficient and secure to share the highly confidential documents

10. CONCLUSION:

We used two layer QR code. This 2LQR code is of two levels namely public level and private level.

The public level QR code can be read by any QR code reading application. But the private level QR code needs a specific application with specific input information. And this private level QR code is created by replacing black modules along with some specific textured patterns. Any standard QR code reader consider the textured pattern as a black modules thus the private level is invisible to standard QR code readers and this private level QR code does not affect any of the public levels

REFERENCES

1) Xiaojun Chen and Jea H. Choi. (2010), 'Security and Privacy in Mobile Social Networks: Challenges and Solutions'13 Volume 3, No. 1.

2) HsinyiPeng and Po-Ya Chuang. (2012), 'Ubiquitous Performance-support System as Mind tool: A Case Study of Instructional Decision Making and Learning Assistant' Educational Technology & Society, 12 (1), 107–120.

3) M. C. Mayorga Toledano. (2006), 'Learning objects for mobile devices: A case study in the Actuarial Sciences degree' Current Developments in Technology-Assisted Education

4) Z. Baharav and R. Kakarala.(2013), Visually significant QR codes: Image blending and statistical Analysis. In Multimedia and Expo (ICME), IEEE International Conference on, pages 1–6.

5) C. Baras and F. Cayre. (2012),2D bar-codes for authentication: A security approach. In Signal Processing Conference (EUSIPCO), Proceedings of the 20th European, pages 1760–1766.

6) T. V. Bui, N. K. Vu, T. T.P. Nguyen, I. Echizen, and T. D. Nguyen.Robust message hiding for QR code.(2014) In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Tenth International Conference on, IEEE pages 520–523.

7) B. A. M. Hoang, W. Sawaya, and P. Bas.(2014) Documentauthentication using graphical codes: Reliable performance analysis and channel optimization. EURASIP Journal on Information Security.

8) T. Langlotz and O. Bimber.Unsynchronized 4D barcodes.(2007) In Advances in Visual Computing, Springer, pages 363–374.

9) C.-Y. Lin and S.-F.Chang. (1999) Distortion modeling and invariant extraction for digital image print-and-scan process.In Int. Symp.Multimedia Information Processing.

10) P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen. (2013) Secret hiding mechanism using QR barcode. In Signal-Image Technology & Internet- Based Systems (SITIS), IEEE, International Conference on, pages 22–25.

BIOGRAPHIES

J. Sharon Chella Priyanga is PG Student at Anand Institute of Higher Technology at Chennai

Her area of interest includes Data mining, Cloud computing, cryptography.

A,S Balaji is presently working as a Assistant Professor in Anand Institute of Higher Technology at Chennai.

His area of interest includes Computer networks and Security, Cloud computing, Wireless sensor networks and Software Engineering etc.