International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

SENSITIVE DATA SHARING USING QRCODE

T. Divya Bharathi[1], G. Iswaryah[2], M. Narmadha[3], R. Kapila Vani[4]

[1,2]STUDENT, DEPT OF CSE, PRINCE SHRI VENKATESHWARA PADMAVATHY ENGINEERING COLLEGE,
[3]ASSISTANT PROFESSOR, DEPT OF CSE, PRINCE DR.K. VASUDEVAN COLLEGE OF ENGINEERING,
[4]ASSISTANT PROFESSOR, DEPT OF CSE, PRINCE SHRI VENKATESHWARA PADMAVATHY ENGINEERING COLLEGE

ABSTRACT - *In this paper, we are proposing an application called QRDROID for sharing sensitive information using cloud storage services. The user can remotely upload their data to the cloud and utilize the data sharing capability with others. In some cloud storage system, cloud file may contain sensitive information. Remote data integrity auditing is proposed to guarantee the integrity of the data stored in the cloud. Encrypting the whole shared file may hide sensitive information, but will make the shared file unusable. A remote document reference id will automatically convert to a QRCode that can be scanned. The user can then download the document without compromising sensitive information at the same time use the data sharing capability. Signatures are used to verify the file in the phases of integrity auditing.*

INTRODUCTION

The audit file mainly associated with gaining information about financial systems and the financial records of the company or business. A financial audit is performed to ascertain the validity and reliability of information, as well as to provide an assessment of a systems internal control. As a result of this, a third party can express an opinion of the persons/organization/system etc. the opinion given on financial statements will depend on the audit evidence obtained. There are also new types of integrated auditing becoming available that use unified compliance material. The auditors of financial statements and non- financial information's can be classified into three categories as an external auditor, cost auditor, secretarial auditor.

In the existing system, the auditor will audit the information, when an auditor audits the accounts are inspected key financial statements of a company, the findings are usually put out in a report or complaint in a systematic manner. During the auditing process, a lot of papers are used. In the existing systems, all the works are done manually.

Enabling identity-based integrity auditing and data sharing with sensitive information hiding for safe cloud storage in some common cloud system such as the electronic help recorders system, the cloud file might contain some sensitive information. The sensitive information should not be open to others when the cloud file is share private key correctness to ensure that when the pkg sends a private key to the user, this private key can pause the verification of the user. The correctness of the unseeing file and its corresponding signature to guarantee that when the user sends an unseeing file and its valid signature to the refiner, the unseeing file and its corresponding signatures he generates can pass the verification of the refiner. Auditing correctness to ensure that the cloud properly stores the user's refined data, the proof it generates scan can pass the verification of the TPA.

User-Level Runtime Security Auditing for the Cloud In our current generation, cloud computing is important over the IT solutions by providing ubiquitous, on-demand access and convenient over the shared pool of resources. It overcomes transparency and accountability through security auditing technology. According to auditing in the cloud make some challenges in collecting the data and verifying it and also cause heterogeneity in cloud infrastructure. Till now there is no means of time to verify the security over the larger cloud. Hence in this paper, we propose runtime security auditing over cloud which concentrates on the user side by providing access control and authentication as RBAC, SSO etc. Here we make use of the open stack to manage the cloud system. The main idea is to reduce the response time at a practical level, it is a costly operation that is done only once and also it is an efficient incremental runtime verification. The final results obtained is realistic under this approach.

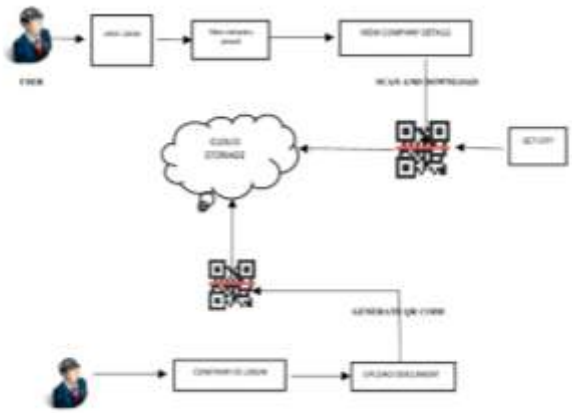
Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage. It provides on-demand outsourcing data services for both organizations and individuals. It uses storage based on a dynamic hash table (DHT), which is a new two-dimensional data structure located at a third party auditor (TPA) to record the data property information for dynamic auditing. In this, the authorized information migrates from the CSP to the TPA. Public auditing: anyone is allowed to have the capability to verify

the correctness and integrity of the user's data stored in the cloud. Storage correctness: the CSP, which does not correctly store users' data as required, cannot pass the verification. Block less verification: no data block needs to be retrieved by the TPA during the verification process. Dynamic data auditing: dynamic data operations should be supported while efficient public auditing is achieved. Privacy-preserving: the TPA cannot derive any actual content of users' data from the received auditing information. Batch auditing: the TPA can handle multiple auditing tasks from various users in a fast and cost-efficient manner. Lightweight: the verification should be performed with the minimum communication and computation overhead.

Trust is good, control is better: creating secure cloud by continuous auditing Many organizations make outsourcing their data, business process and application over the cloud. On – demand provisioning and pay -per use pricing is done over financial and technical benefits. Cloud Service Certification provides high level of security and compliance. The cloud services provide multiple validity period which may put in doubt of such certification. We argue that the continuous auditing (CA) is required to have a reliable and security cloud services, where the existing criteria are not applicable for the third - party auditing process. Hence here we purpose a conceptual architecture in which they link the applicable internal and third party auditing methodology for auditor and providers.

Identity – based data outsourcing with comprehensive auditing in cloud For the distributed client the cloud storage system provides a file sharing and storage. Identity based data outsourcing (IBDO) scheme provides integrity, controllable outsourcing over the files. Our IBDO scheme allows user to authorize dedicated proxies to upload data over the cloud storage server, the proxies are identified and authorized by the identities which eliminate complicated certificate management. IBDO also facilitates comprehensive auditing i.e., not only permits regular integrity but also to audit the information on data origin, type and consistence of outsourced files .Thus security analysis and evaluation tells our IBDO provide strong security and an efficient one.

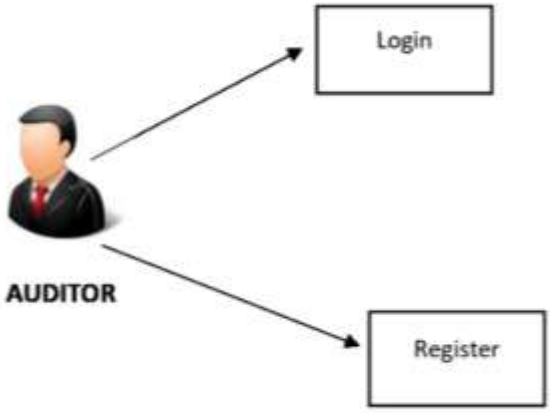
ARCHITECTURE:



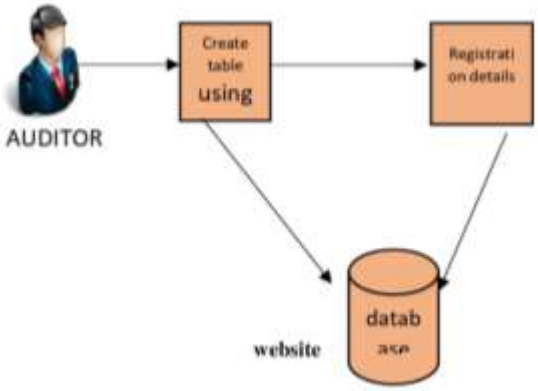
The above figure describes how the auditor uploads the file of a particular company onto the cloud. Initially, the auditor signs up and logs into the website using company id, company name, mobile number, and password. The auditor then uploads a particular file. The file may be of any format like text, doc or jpeg or any other document type. The uploaded document is encoded with the QR Code and stored in the cloud. The User then, logs in to the website with the help of the company id and password. Once the user logs in, the company details are displayed. The user then selects the file that has to be downloaded from the cloud. The unique QR Code that was previously generated is displayed on the screen. The User scans this QR Code. As part of the verification process, an OTP is generated and sent to the User's mobile number. The User enters the OTP in the app. Once the verification is successful, the file is downloaded onto the mobile. Once the User completes his work on the file and chooses to delete the file, the file is deleted only from the mobile but not from the cloud.

Login and register on the website **-** In this module, we designed to develop a signup and login screen. In this first, the auditor will sign up with all the details like company ID, company name, address, phone number, and password**.** These information's will be stored in the database. After signup then it will move to the login page. The login page contains company ID and

password, the auditor input will be verified with the data in the database and move to the next page. These websites are created using HTML, CSS etc., and for the database, we use PHP and my SQL.



Once the Auditor has entered the company id and password during registration, the website uses PHP to create the database for storing and fetching auditing details.

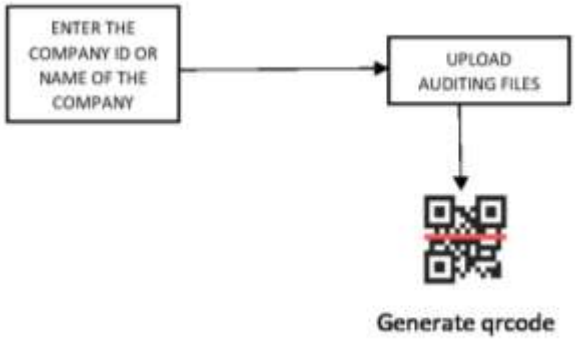


QR code generation and file upload After login, the website will move to the next page which contains information about the company name, company ID, address, phone number and creates QR Code. This creates a QR Code will create a unique QR CODE (quick response code). Then the auditor will select the file which has to be uploaded.

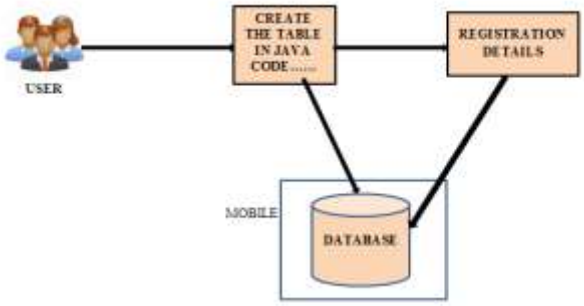
The QRCode is generated by using the API

```
//getting link for image

public function get_link($size = 150, $EC_level = 'L', $margin = '0'){

$this->data=urlencode($this->data);
Return'http://chart.apis.google.com/chart?chs='.$size.'x'.$size.'&cht=qr&chld='.$EC_level.'|'.$margin.'&chl='.$this->data;

}
```

This API consist of three major part the first part describe about the size of the QR Code. The second part describe about the levels of error detecting, there are four levels in QR code generation they are L,M,Q,H.

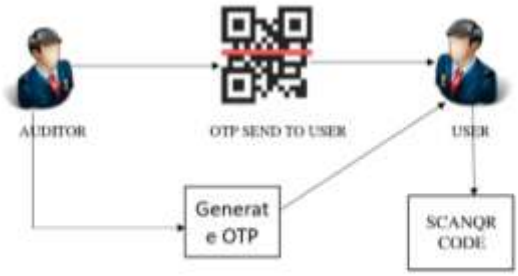


Registration and log in on the mobile application this module focus on the design to develop signup and login page for the user. The signup contains normally user ID or Email ID, password and confirms the password. These registration details are stored in the database. After signup, the user will be automatically navigated to the login page which contains user ID or Email ID and password. This module designed and developed based on android and java and for the database, we use my SQL. This module is mainly based on the use of perspective. Login page if the user ID or Email ID and password then the application allows the user to log in or else the application will display an alert message to the aliduser.



Scanner and OTP generation and file download this module is based on scanners. This application we use a special type of scanner call QR droid. QRdroid is used to scan any type of user QR Code. Initially, auditor generates The QR code and sent to the authorized user. Then the user will scan the QR code and retrieve the key and at the same time, an OTP (ONE TIME PASSWORD) is generated to the registered mobile number of the user. The OTP is used to increase privacy and security. After validating the OTP the particular file which the user wants will be downloaded from the cloud.

File Download -Once the Key is retrieved from the auditor, this key is used to fetch the file from the server. Then the user can easily access the file that are stored in the cloud.



CONCLUSION:

This project is mainly used to reduce the paper work and reduce the storage made by them.it also increase the security and increase the privacy of sensitive information that are stored in the cloud.

FUTURE CONCEPT: - In future there will more advanced like artificial intelligence. Human Segmentation Algorithm can be used 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 modeled with spatial color Gaussian mixture models (SCGMMs).

Reference Paper:

1) ISO/IEC 15420:2009. Information technology - Automatic identification and data capture techniques - EAN/UPC bar code symbology specification. 2009.

2) ISO/IEC 16022:2006. Information technology - Automatic identification and data capture techniques - Data Matrix bar code symbology specification. 2006.

3) ISO/IEC 18004:2000. Information technology - Automatic identification and data capture techniques - Bar code symbology - QR Code. 2000.

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

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

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

7) A. T. P. Ho, B. A. M. Hoang, W. Sawaya, and P. Bas. Document authentication using graphical codes: Reliable performance analysis and channel optimization. EURASIP Journal on Information Security, 2014(1):9, 2014.

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

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

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