SECURE3 AUTHENTICATION FOR SENSITIVE DATA ON CLOUD USING TEXTUAL, CHESSBOARD AND QR CODE PASSWORD SYSTEM

V. R. Waghmare[1], Bhushan Shinde[2], Pankaj Patil[3], Puja Kasbe[4], Sharad Ghodake[5]

[1]IT, Savitribai Phule Pune University, India, (MMIT, Lohgaon)
[2]IT, Savitribai Phule Pune University, India (MMIT, Lohgaon)
[3]IT, Savitribai Phule Pune University, India (MMIT, Lohgaon)
[4]IT, Savitribai Phule Pune University, India (MMIT, Lohgaon)
5IT, Savitribai Phule Pune University, India (MMIT, Lohgaon)

Abstract

Existing systems of authentication are plagued by many weaknesses. As a high speed cloud infrastructure is being developed and people are informationized, the sensitive data are also engaged in cloud feild. However, the existing cloud sensitive file upload and download on cloud was exposed to the danger of hacking. Recently, the personal information has been leaked by a high degree method such as Phishing or Pharming beyond snatching a user ID and Password. Seeing that most of examples which happened in the file uploading and downloading were caused by the appropriation of ID or Password belonging to others, a safe user confirmation system gets much more essential. In this paper, we propose a new authentication system file uploading and downloading on cloud using HADOOP technique. In HADOOP technique there are 3 technique but we can use HDFS (Hadoop Distributed File System).This authentication system is a combination of a three authentication system i.e. Secure3 in that 1)Textual,2)Chessboard,3)QR-code Authentication. In Textual authentication normal authentication is required to login .i.e username and password. In chessboard authentication user plays a steps of a chessboard and select that steps as authentication. In QR-code used Mobile OTP with the combination of QR-code which is a variant of the 2D barcode. we also include a priority of a sensitive data in that low priority sensitive data have only a Textual authentication system. Medium priority sensitive data have Textual +chessboard authentication system. High priority sensitive data have Textual +chessboard +QR-code authentication system.

Keywords: *OTP(one Time Password),QR(Quick-Response),CBS(Chess Board System),HDFS (Hadoop Distributed File System),IMEI(International Mobile Center Equipment Identity),AES(Advanced Encryption Standard).*

--***--

1. INTRODUCTION

File uploading and downloading is most sensitive task performed by general internet User. In this paper, we propose authentication system for sensitive data uploading and downloading on cloud based hadoop Distributed File System(HDFS).Cloud network which can provide greater security and convenience to user for sensitive information by Secure 3 authentication system i.e. textual password, chessboard system and mobile OTP with the QR-code. Once the user enter a textual password it matches with the users original password if it correct then user goes to chessboard authentication. In chessboard authentication user plays a chess game on one side and opposite side moves automatically plays by AI system and stores the playing moves password in a database. Only user moves are stored as a password. When user login to his account this time he play this moves again if this moves is match with database stored moves then he goes to QR code authentication. QR code authentication is very secure system in that OTP is used. OTP is a combination of a user mobile IMEI no and a selected random number. OTP is send on users mobile. In QR code users mobile IMEI no is added with random no between (0-9999) this number store in database.

2. RELATED WORK

Authentication is accepting proof of identity given by a credible person who has evidence on the said identity or on the originator and the object under assessment as his artifact respectively. Traditional authentication technique generally requires an id and password to verify the identity of user. By nature, user is looking for a password that is easy to remember and secured from any attack. However, remembering many complicated passwords, especially when user has different accounts, is not an easy task. Earlier two factor authentication technique is common in use. In the two factor authentication individual can be identified by his user name and password. If username and password is matched then process of authentication is done and user can access the data. But in this technique anyone can hack password and access information. In many cases, users' passwords are stored in plain-text form on the server machine. Anyone who can gain access to the server's database has access to enough information to impersonate any authenticable user. In cases in which users' passwords are stored in encrypted form on the server machine, plain-text passwords are still sent across a possibly-insecure network from the client to the server. Anyone with access to the intervening network may be able to "snoop” pairs out of conversations and replay them to forge authentication to the system. Each separate system must carry its own copy of each user's authentication information. As a result, users must maintain passwords on each system to which they authenticate, and so are likely to choose less-than-secure passwords for convenience. Knowledge based authentication uses secret information. When user provides some information to authenticate himself as a legitimate user, the system processes this information and suggests whether the user is legitimate or not.

3. PROBLEM STATEMENTS

In this paper, we propose a new authentication system file uploading and downloading on cloud using HADOOP technique(HDFS).This authentication system is a combination of a three authentication system i.e. Secure3 in that 1)Textual,2)Chessboard,3)QR-code Authentication. In textual authentication is required to login .i.e username and password. In chessboard authentication user plays a steps of a chessboard and select that steps as authentication. In QR-code used Mobile OTP with the combination of QR-code which is a variant of the 2D barcode. We also include a priority of a sensitive data in that low priority sensitive data have only a normal authentication system. Medium priority sensitive data have textual +chessboard authentication system. High priority sensitive data have textual +chessboard +QR-code authentication system. The following requirements are satisfied in the proposed scheme .

1. The new scheme provide secrets that are easy to remember and very difficult for intruders to guess.
2. The new scheme provides secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others.
3. The new scheme provides secrets that can be easily revoked or changed

4. OBJECTIVES

4.1 Authentication

We provide 3 authentication system i.e. Textual, Chess Board and QR Code password system.

4.2 Registration

In this authentication system we provide user registration in that users details, (i.e. UserID ,LoginName, FullName, MobNo, IMEINo) and play chess board moves for password. This information and password stored in database at the time of registration.

1. **File Upload:-**
   File send and upload user itself and compose to other user. For upload a file on cloud we can provide priorities on the basis of importance of data. And HDFS Techniques.

2. **File Download:-**
   File download by user itself using a hadoop distributed file system.

3. **File Encryption:-**
   We provide encryption algorithm i.e. AES for textual password. This algorithm provides more security for textual password.

4. **File Decryption:-**
   We provide decryption algorithm i.e. AES for textual password. This algorithm provides more security for textual password.

5. **QR Code Encoder/Decoder:-**
   QR code encoder and decoder is used to encode and decode the QR code.

6. **Chess Board Environment:-**
   User play a moves of a chessboard at the same time AI player also play a chessboard game but only user game is stored in database in encrypted format.

5. PROPOSED WORK AND METHODS

Here the designs secure3 system of two 3D environments are specified ,and one normal environment is specified. The first is a normal authentication system the second one being a chess game and the third being a OTP with QR code. In the chess game, the password is based on placing the chess pieces in predefined positions on the chess board and in the case of the QR code, the password is constructed base on mobile IMEI no. adding a random number(0-9999)on mobile IMEI no.

5.1. Environment1-Textual Login:

When a new user enters in the environment, the user must initially enter all users details in the registration form. The user must then click on the CHECK LOGIN button to select the chess environment. Figure1 below shows an environment for a Textual-Login, having its username and password. Password should contain character, number and special symbols.

5.1.1 Encryption

The process of converting plain text to cipher text is known as encryption. In this system the password of that user will send or receive will be in encrypted format. To achieve this we will be using AES (Advanced Encryption Standard) algorithm which is advanced version of DES (Data Encryption Standard).The main advantages of AES are that its resistance against all known attacks; speed and code compactness on a wide range of platforms; design simplicity .

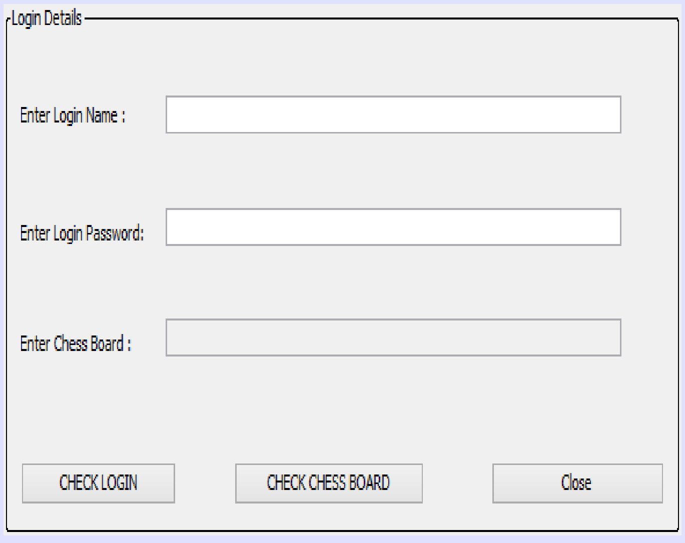


Fig 1:-Textual Login

5.1.2 Decryption:

The process of converting Cipher text to Plain text is known as Decryption. In this system the password of that user will be receive in Decrypted format. To achieve this we will be using AES (Advanced Encryption Standard) algorithm which is advanced version of DES (Data Encryption Standard).The main advantages of AES are that its resistance against all known attacks; speed and code compactness on a wide range of platforms; design simplicity .

5.2. Environment 2 – Chess Board

When a new user enters the environment, the user must initially enter all user details in the registration form. As well as user plays a moves of a chessboard this moves and user details are stored in database. The user must then click on the CHECK LOGIN button to select the chess environment. Figure2 below shows an environment for a chess game, having a total of 32 objects, out of which 16 are red and 16 are white. It also encloses three buttons all together namely, start game, stop game, and close the game.

5.2.1 Encryption

Encryption algorithm is used for encrypting a chessboard password. We are using a AES for encrypting a chessboard password.

5.2.2 Decryption

Decryption algorithm is used for decrypting a chessboard password. We are using a AES for encrypting a chessboard password.

Each button works as specified below:-

1. Start Game:-

This button can be used by user to start playing of chessboard game at the registeration time and at the login time of a user. Once this button is clicked, the user can moves the chessboard objects.

2. Stop Game:-

This button is used to end the sequence of actions and interactions. Clicking this button stops recording the users movements and the recorded actions and interactions are saved as a 3D password in the form of a string.

3. Close:-

Once clicked, the environment is closed and control returns to the registration form. Following diagram shows how actual ChessBoard password is stored in the database. ChessBoard password is stored matrix format in a database. Source and destination point of a object is selected as a password of one moving object. Same as a second moving object. This process is continuous till last moving object. This password is stored in a encrypted format in a database.

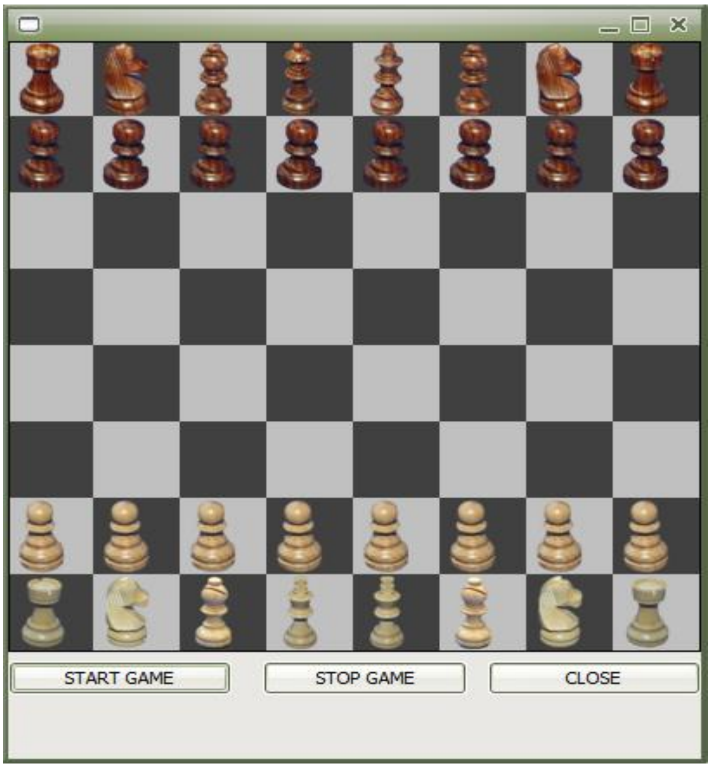
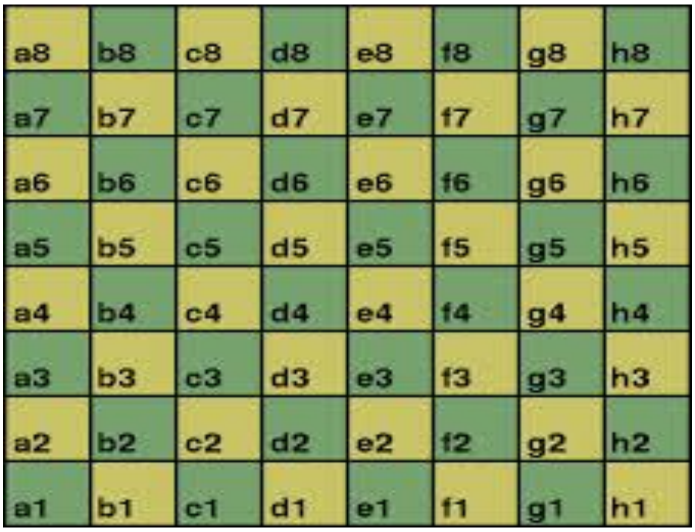


Fig 2:- ChessBoard Login



a8	b8	c8	d8	e8	f8	g8	h8
a7	b7	c7	d7	e7	f7	g7	h7
a6	b6	c6	d6	e6	f6	g6	h6
a5	b5	c5	d5	e5	f5	g5	h5
a4	b4	c4	d4	e4	f4	g4	h4
a3	b3	c3	d3	e3	f3	g3	h3
a2	b2	c2	d2	e2	f2	g2	h2
a1	b1	c1	d1	e1	f1	g1	h1

Fig 3:-PWD Matrix format of chessboard

5.3 Environment 3 –QR Code

5.3.1 OTP and QR Scanner

An OTP is a generated password which only valid once and QR Scanner is an android application for scanning QR Code. The users mobile that can generate an OTP using an algorithm of permute string and cryptographic keys by scanning the QR code by the QR Scanner. On the server side, an authentication server can check the validity of the password by sharing the same algorithm and keys. Mobile QR Code Scanner application can be used to generate the OTP, The OTP is a combination of a user mobile IMEI-NO and randomly selected number. Any random number is added on a users mobile IMEI no. This password is valid only one time. To generate a OTP permute string algorithm logic is used to send a OTP.

5.3.2 QR_Code

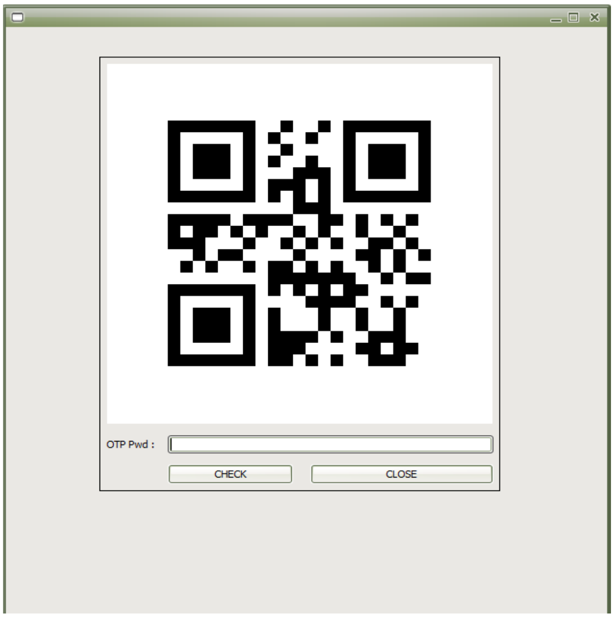


Fig 4:-QR Code Login

There are two buttons are used in a QR code:-
1. Check:-
This button is check whether user enter OTP is correct or not.

2. Close:-
This button is used to close the QR-Code environment.

5.3.3 Structure of QR-Code

QR code (abbreviated from **Quick Response Code**) is the trademark for a type matrix barcode(or two-dimensional barcode). A QR code uses four standardized encoding modes (numeric, alphanumeric, byte / binary) to efficiently store data; extensions may also be used The QR Code system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC Barcode . Applications include product tracking, item identification, time tracking, document management, and general marketing.. A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Reed error correction until the image can be appropriately interpreted. The required data are then extracted from patterns present in both horizontal and vertical components of the image.

Fig 5:-QR Code.

5.4 File Upload and Download using HDFS

We use HDFS for uploading and downloading file on cloud for more security .HDFS means Hadoop Distributed File System is more useful for to produce the bulk filename of the uploaded file on cloud server. For that we can provide more security to the our personal information or data on the cloud storage. HDFS has a master/slave architecture.HDFS cluster consists of a single Name Node, a master server that manages the file system namespace and regulates access to files by clients. In addition, there are a number of Data Nodes, usually one per node in the cluster, which manage storage attached to the nodes that they run on. HDFS exposes a file system namespace and allows user data to be stored in files. Internally, a file is split into one or more blocks and these blocks are stored in a set of Data Nodes. The Name Node executes file system namespace operations like opening, closing, and renaming files and directories. It also determines the mapping of blocks to Data Nodes. The Data Nodes are responsible for serving read and write requests from the file system's clients. The Data Nodes also perform block creation, deletion, and replication upon instruction from the Name Node.

5.5 QR Code Scanner

We take a application of QR code scanner and in capture activity develop a algorithm of permute string. This same algorithm is developed in login code of a client side. A OTP. is a combination of a beginning string +ending string. Beginning string is a IMEI no and ending string is an random number

5.6 HDFS (Hadoop Distributed File System)

We create a HDFS virtually in the system. We install HDFS in linux OS.

5.7 Architecture of Proposed System

The proposed system have required first user registration. In user registration required users login name and password is stored in the database at the time of a registration. As well as in the time of registration user play a chessboard game and this chessboard moves also stored in a user database. The user registration nothing but a personnel information of a user. When this information is fill then user account will be created. Then user do their personnel work like file uploading and downloading of a sensitive data on cloud using HDFS. The proposed system is more secure than a other authentication system. The proposed authentication system requires a three step authentication.

First authentication is normal. In textual authentication user requires his username and password at the time of login. If user entered username and password is correct then he moves from chessboard otherwise he display a message incorrect username or password. After completion of first environment user goes to a chessboard environment in this environment he plays a chessboard moves played moves is matches with the database stored password. When this moves is correct he goes to a QR code environment otherwise he goes to a normal login. After completion of a chessboard user goes to a QR code environment in that environment user requires a OTP. When this password is correct then user have a permission to do their work(File Uploading and File Downloading)on cloud using a hadoop framework.

Algorithm of QR Code Scanner

```
1. Start.
2. Accept beginning and ending string.(i.e. IMEI no and selected random no.)
3. If ending string <=1 thengotostep5
4.OTP=BigInteger.valueOf((Long.valueOf(beginningString)) + Integer.parseInt(endingString));
5. else
for (int i = 0; i <= endingString.length(); i++) Increment a ending string one at a time
6. Original OTP=ipermuteString(beginningString + endingString.charAt(i), newString);
7. Stop.
```

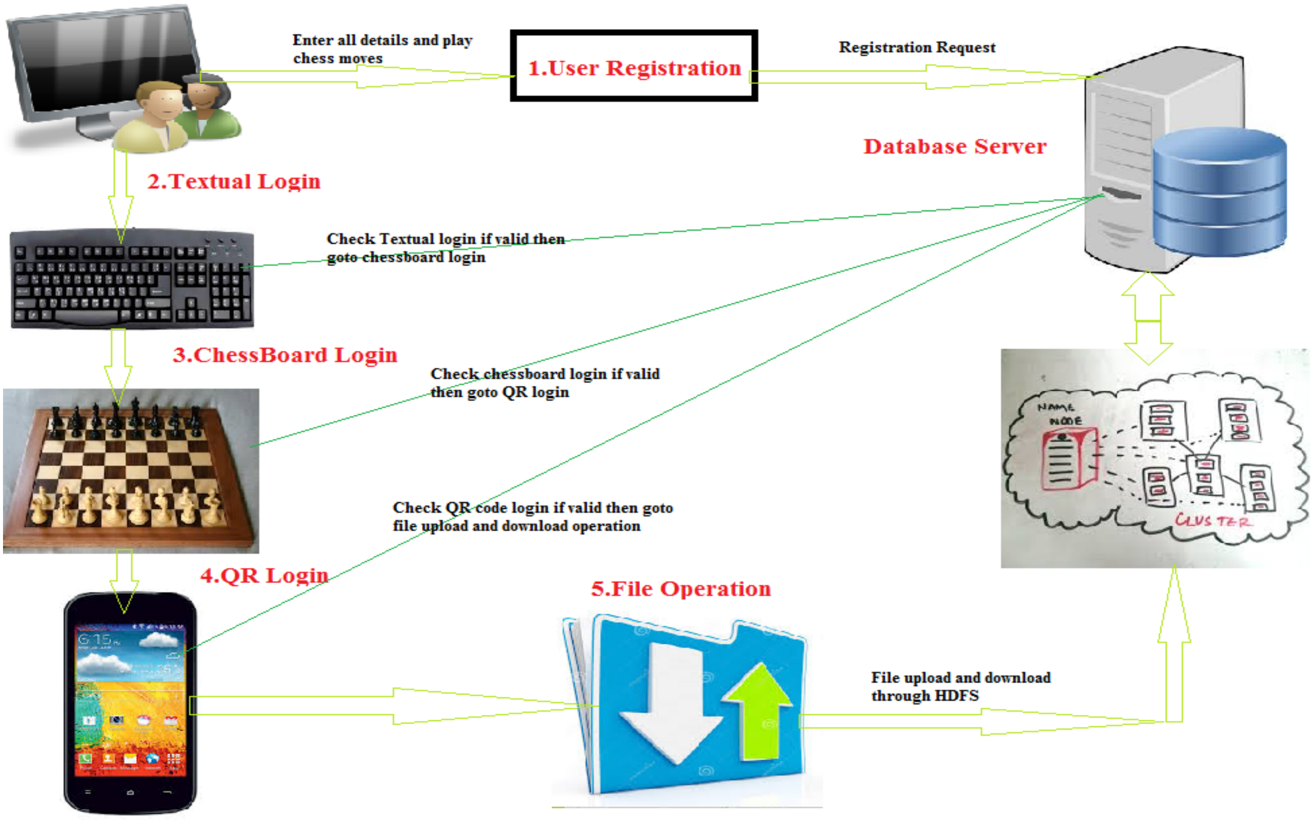

Enter all details and play chess moves
1.User Registration
Registration Request
Database Server
2.Textual Login
Check Textual login if valid then goto chessboard login
3.ChessBoard Login
Check chessboard login if valid then goto QR login
Check QR code login if valid then goto file upload and download operation
4.QR Login
5.File Operation
File upload and download through HDFS
NAME NODE
CLUSTER

Fig 6:-System Architechture

6. ADVANTAGES

1. It is more secure system.
2. Used for sensitive data.
3. Used to store personnel information on cloud.
4. Three authentication system is used so it is more secure than other authentication system.

7. BENIFITS OF PROPOSED SYSTEM

1. Critical server many large organizations have critical servers that are usually protected by a textual password. A secure 3 password authentication proposes a sound replacement for a textual password.
2. Nuclear and military facilities such facilities should be protected by the most Powerful authentication systems. The secure 3 password has a very large probable password space, and since it can contain token, biometrics, recognition and knowledge based Authentications in a single authentication system, it is a sound choice for high level security locations.
3. Airplanes and jet fighters Because of the possible threat of misusing airplanes and jet fighters for religion, political agendas, usage of such airplanes should be protected by a powerful authentication system. In addition, 3D passwords can be used in less critical systems because the 3D virtual environment can be designed to fit to any system needs.
4. A small virtual environment can be used in the following systems like
    4.1 Personal Digital Assistance
    4.2 Desktop Computers laptop logins
    4.3 Web Authentication
    4.4 Security Analysis

8. CONCLUSION

We proposed a system called Secure 3 authentication system using textual, chessboard , and QR code password system. In this we provide 3 authentication system step by step (one level after another level).

First we provide a user registration for new user. In user registration all user details is _lled by user. In the time of user registration chessboard password moves will be saves in a database. First level of authentication is a textual login. In textual login we provide username and password that password is stored in database in encrypted format. We have use a AES algorithm for encryption and decryption of textual password. Second level of authentication is chessboard authentication. If user enter a username and password is correct then he goes to chessboard login. In chessboard login user plays a moves of chessboard that move store in database in matrix format. Third level of authentication is QR code login. In QR code we have use a 2D barcode format. QR code is captured by QR code scanner this password 68 is only valid for only one time. QR code password is a combination of a user IMEI no and a random number. The random number is between the (0-9999). We give one QR code scanner android application from google apps and developed a one algorithm in that application i.e Permute String. Permute string is a combination of a IMEI no and a selected random number from(0-9999).

We use HDFS (hadoop distributed _le system) for _le uploading and downloading from cloud. Bulk name is assigned for every _le in HDFS. Our systems provide the security or authentication for sensitive data as the hacker will have to go through three levels of authentication in which the complexity level increases at every step.

REFERENCES

[1]. William Stallings, "Cryptography and Network Security: Principles and Practice", Sixth, 2013.
[2]. William Stallings, "Cryptography and network security", Sixth, 2013.
[3]. Mohammad Mannan, P. C. Van Oorschot, "Security and Usability: The Gap in Real-World Online Banking", NSPW 07, North Conway, NH, USA, Sep. 18-21, 2012., 175-191.
[4]. Anti Phishing Group, Phishing Activity Trends Report , from: http://www.antiphishing.org, Dec. 2008.
[6]. Sang-Il Cho, Hoon Jae Lee, Hyo-Taek Lim, Sang-Gon Lee , OTP Authentication Protocol Using Stream Cipher with Clock-Counter, October,2009.
[7]. Jean-Daniel Aussel, Smart Cards and Digital Identity , Telektronikk 3/4. 2010. ISSN 0085-7130.
[8]. Jose Rouillard, Contextual QR Codes , Proceedidngs of the Third International Multi-Conference on Computing in the Global Information Technology (ICCCGI2008), Athens, Greece, July 27-Augst 1, 2012.67
[9]. IETF RFC 4226, HOTP: An HMAC-Based One-Time Password Algorithm, Dec. 2011,
[10]. ISO/IEC 16022:2000, Information Technology International Symbology Specification Data Matrix, 2008.