www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 5 May 2017, Page No. 21230-21235
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i5.08

E-KYC Ticketing System

Yogesh Suman[1], Ms. G.Geetha[2]
[1]SRM University,
Kattankulathur Kancheepuram,Chennai
Yogeshsuman166@gmail.com
[2]SRM University,
Kattankulathur Kancheepuram,Chennai
Geetha.g@ktr.srmuniv.ac.in

Abstract: The e-KYC ticketing system is the new way to book the tickets like bus ticket, train ticket, flight ticket, and other ticket bookings. The main purpose of the e-KYC ticketing system is to ensure the safe and secure journey of oneself and other fellow passengers.

The e-KYC ticketing System is a new way to verify the passengers having journey on bus, train, flight etc. The e-KYC system permits ticket booking to the verified passengers only. This system will ask the Universe Identity Number as we have universe identity in India like Aadhar Card. Without the Aadhar card people will not be able to travel by any mode of transport.

The e-KYC ticketing system uses two way verifications. The first verification happened before booking the ticket. The user needs to give his Aadhar card number to register them on the website. If they are not having Aadhar card then they cannot book the ticket. The second verification takes place when the TT comes to check the ticket. Her e TT will be having a device which will ask the ticket number and the thumb impression of the passenger. This thumb print will be matched with the existing database. If it match then he can travel in the train else an e-mail will be sent to railway department and the journey of the particular pass anger will be denied.

1. Introduction

E-KYC ticketing system is railway ticket booking system. This system uses the unique identity of passengers given by the government of India. This unique identity is the Aadhar card of the person. Here we will be using the Aadhar card to cross check whether the passenger is an authorized passenger or an illegal person travelling on someone else ticket.

Here the passenger should sign up on the ticketing booking website. The passenger
needs to have an Aadhar card provided by the government of India. After all this the registration or sign up will be completed.

Now the passenger can select the desirable journey on railway system. Here the
passenger needs to select the journey date, source station and the destination station as well as the passengers can select the train in which they want to have their journey and here passenger can also choose the number of seats and type of seats like third as, second ac, first ac, sleeper coach, chair car, second seating etc.
Now the most important part of this project is to verify the passenger during g their
journey. Now at this point of time the TT will enter their ticket number and he will ask to give thumb impression on the device. Now this thumb impression will be matched with the pre existing database of Aadhar card.

This is a biometric based system which uses Aadhar Card for the reservation system to identify the right passenger and the wrong person. Biometric authentication is an automated method of recognizing a person's identity. Biometric authentication can be classified into unimodal and multimodal biometric systems [1]. Unimodal systems use single biometric traits whereas Multimodal biometric system makes use of different biometric traits simultaneously to authenticate a person identity. In the existing system we have no security of the fellow passengers as we cannot identify the fraud person. Now a days the government is planning to have Aadhar based reservation only for senior citizen, but what about other age people. Many of the fraud people come under the age group 18-35. So this should be for every person.

The railway ministry has already included Aadhar as a means of verification in the
Tatkal booking system. Tatkal is the emergency ticket system. The Tatkal ticket can be booked before 24-48hr of the journey. The Aadhar is used for the current ticket booking system. The Aadhar card is a universal identity of every Indian. This identity card contain the details like name, father name, complete address, mobile number and the biometric details of the person like iris pattern, all finger impression and the thumb impression etc. This is a unique 12 digit number provided by the government of India.
So this system will deal with the Aadhar card database of the individual and it will
be used for the reservation of the ticket through online and then the individual will be required to show his/her Aadhar card at the railway counters for verification. Indian Railway has already started the procedure for the implementation of the scheme but only for senior citizens. The TT will carry a device along with him which will be having all the details of the passengers whoever is travelling in the train. The device will be used to verify the passenger details by taking the thumb impression and then thumb impression will match the details of the passenger stored in the device. If the device fails to identify the impression than it is clear that the person who is travelling has used a fake identity while doing reservation of the tickets.

This complete system will be examined by officials at all the times and even there is no chance that the TT can take money from the passenger.
Aadhar card will be used in two phases-
1. Sigh Up on the website.
2. TT verification.

During signup the Aadhar card number is required. Everyone must have Aadhar card to book the ticket. At the time of TT verification along with ticket number the
thumb impression is also required to match will Aadhar card database.

The e-KYC ticketing system will be the safe and secure system for the railway reservation system. With this system we can be sure that no passenger can travel without ticket, without Aadhar card and the most important is no one can even travel on behalf of someone else on someone else ticket.

Fingerprint Technology

The fingerprint is the biometric identity of the human beings. As all the human are differ from their biometric like fingerprints, eye etc. So the finger print…biometric can be the best way to ensure the security of any system. So this can be implemented in any field.[3]

Figure 1: - Finger Prints taken from the sensor

If we talk about fingerprints, a fingerprint is the feature pattern of one finger (Figure1). It is an impression of the friction ridges and furrows on all parts of a finger. These ridges and furrows present good similarities in each small local window, like parallelism and average width.
However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by the technique called image encryption.

Fingerprint matching techniques

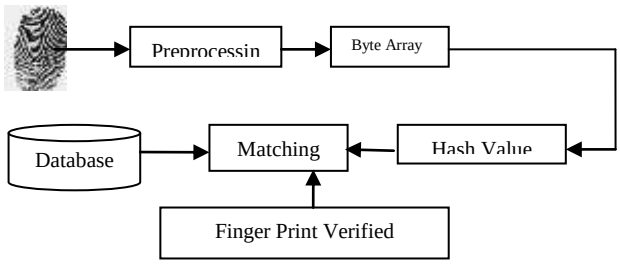
The large number of approaches to fingerprint matching can be coarsely classified into three families.

- **Correlation-based matching**:-In this type of matching Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments like. various displacements and rotations.
- **Minutiae-based matching**:- This is the most popular and widely used technique. It is being the basis of the fingerprint comparison made by fingerprint examiners. The minutiae are extracted from the two fingerprints and stored as a sets of points in the two-dimensional plane. Minutiae-based matching consists of finding the alignment between the template and the input minutiae sets that result in the maximum number of minutiae pairings.
- **Pattern-based matching**:- This is also called image based matching. Pattern based algorithms compare the basic fingerprint patterns like arch, whorl, and loop between a previously stored template and a candidate fingerprint. This technique requires that the images to be aligned in the same orientation. For this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

2. Technology used

In this system will be using an image encryption technique to convert image into string values to verify the finger print of the passenger during TTR verification.
Here in the eKYC Ticketing System we will be using the image encryption technique by following base paper [2].
Here in the project I am using image encryption technique.

Block Diagram



In this technique first we convert the particular fingerprint image to binary formats and after the binary conversion we convert this binary to base 64 strings to make comparisons easy.
Now after this step to match the image we will be using the SHA256 algorithm. This algorithm will check the image size and the image pixels. First the image will be converted into the byte array and then using these algorithms we will calculate has value for the image that will be further compare with the base64 string.
If the image is matched then the passenger fingerprint will be verified else verification failed and in this case an email will be sent to the concern department and the journey will be denied.
There are four side of any finger to be matched, because we can get the print on any angle during verification. Some time the passenger can press one side of his finger or second side on some angle or he may give print upside. So in this case the provided print should be matched. So this can be a good idea to verify all finger prints during the verification process.

Preprocessing

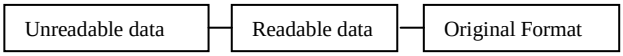
For the image preprocessing we are using base 64 algorithm

Base 64 Algorithm

The base 64 algorithm is groups of binary to text encoding that represent the binary data into the ASCII string format by translating it into radix-64 representation. The term base-64 originates from a specific MIME content transfer encoding. Each base64 digit represents exactly 6 bits of data.

Base64 is a different way of interpreting bits of data in order to transmit that data over a text-only medium,. In the standard 8-bit ASCII character set, there are 256 characters that are used to format text.

We need a way to convert unreadable characters into readable characters and convert them back to their original format.



There are many ways to do this, but the way we are covering now is by using base64 encoding.

The 256 characters in the ASCII character set are numbered 0 through 255. This is the same as 28 , 8 binary placeholders, or a byte. So for any ASCII character, we need one byte to represent this data. As far as a computer is concerned, there is no difference between an ASCII character, and a number between 0 and 255 (which is a string of 8 binary placeholders), only how it is interpreted. Because we are now detached from ASCII characters, we can also apply these same techniques to binary data, for example, a picture, or executable file. All we are doing is interpreting data one byte at a time.

The groups of 6bits are converted into their corresponding Base64 character values.

The problem with representing data one byte at a time in a readable manner is that there are not 256 readable characters in the ASCII character set, so we cannot print a character for each of the 256 combinations that a byte can offer. So we need to take a different approach to looking at the bits in a byte.

There are certainly sixteen readable characters that we could use to represent each variation of nibble. This type of translation is known as hex.

The problem with using hex, is that since we are using one ASCII character (which is, remember, one byte long in storage space) to represent every four bits, anything we translate into hex will be exactly twice as big as the original data. This might not seem like a problem for a small message, but imagine we are trying to send an image or executable. The original size of perhaps a megabyte or more is now doubled. Sending this over email or a slow Internet connection will take twice as long.

The 64 characters we will use are uppercase A-Z (26 characters), lowercase a-z (26 characters), 0-9 (10 characters), '+' (1 character) and '/' (1 character). 26 + 26 + 10 + 1 + 1 = 64, just the number we need. As we can surmise, base64 is still less space efficient than using a full byte, but instead of hex's double space usage, base64 uses only one and a third as much space. In other words for every 3 bytes, we must have 4 base64 characters. All of the characters listed above are easily readable.

Base64 encoding process

The process to encode the input stream is fairly straightforward.

a) The octet stream is read from left to right.

b) Three 8-bits groups within the input stream are concatenated to from a group of 24-bits.

c) Three 24-bits group is further treated as four 6-bits groups that are right justified using zeros. The grouping into 6-bits is for the simple reason that 6 bits will cover the range of printable characters [0-26-1]

d) Each of these 4 groups is then encoded.

Base64 and xml schema

The XML Schema data type library defines a core data type whose value space contains base64 encoded binary data. It is named "base64Binary". This helps facilitate description of binary element content.

Post processing

In the post processing phase here we to calculate the hash value for the images. This hash value is being matched with both the images. If the hash values of both the images are matched it means the finger print images are matched.

So here in this system before booking the ticket the user has to do his Aadhar details registration. After this only he can book ticket. This Aadhar card details will be having finger print that will be converted into base 64 string and will be stored in the database.

Hashing

An n-bit hash is a map from arbitrary length messages to n-bit hash values. An n-bit cryptographic hash is an n-bit hash which is one-way and collision-resistant. Such functions are important cryptographic primitives used for such things as digital signatures and password protection.

Current popular hashes produce hash values of length n = 128 (MD4 and MD5) and n = 160 (SHA-1), and therefore can provide no more than 64 or 80 bits of security, respectively, against collision attacks. Since the goal of the new Advanced Encryption Standard (AES) is to offer, at its three crypto variable sizes, 128, 192, and 256 bits of security, there is a need for companion hash algorithms which provide similar levels of enhanced security.

The cryptographic hash function SHA-256
General description

SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256 bits. It is a keyless hash function; that is, an MDC (Manipulation Detection Code).

A message is processed by blocks of 512 = 16 × 32 bits, each block requiring 64 rounds.

Basic operations

1. Boolean operations AND, XOR and OR, denoted by $\wedge$, $\oplus$ and $\vee$, respectively.
2. Bitwise complement, denoted by -
3. Integer addition modulo 232, denoted by A + B.

DOI: 10.18535/ijecs/v6i5.08

Each of them operates on 32-bit words. For the last operation, binary words are interpreted as integers written in base 2.
4. RotR(A, n) denotes the circular right shift of n bits of the binary word A.
5. ShR(A, n) denotes the right shift of n bits of the binary word A.
6. AkB denotes the concatenation of the binary words A and B.

Functions and constants

The algorithm uses the functions:

Ch(X, Y, Z) = (X ∧ Y) ⊕ (X ∧ Z),
M aj(X, Y, Z) = (X ∧ Y) ⊕ (X ∧ Z) ⊕ (Y ∧ Z),
Σ0(X) = RotR(X, 2) ⊕ RotR(X, 13) ⊕ RotR(X, 22),
Σ1(X) = RotR(X, 6) ⊕ RotR(X, 11) ⊕ RotR(X, 25),
σ0(X) = RotR(X, 7) ⊕ RotR(X, 18) ⊕ ShR(X, 3),
σ1(X) = RotR(X, 17) ⊕ RotR(X, 19) ⊕ ShR(X, 10),

and the 64 binary words Ki given by the 32 first bits of the fractional parts of the cube roots of the first 64 prime numbers:

0x428a2f98 0x71374491 0xb5c0fbcf 0xe9b5dba5 0x3956c25b 0x59f111f1 0x923f82a4 0xab1c5ed5
0xd807aa98 0x12835b01 0x243185be 0x550c7dc3 0x72be5d74 0x80deb1fe 0x9bdc06a7 0xc19bf174
0xe49b69c1 0xefbe4786 0x0fc19dc6 0x240ca1cc 0x2de92c6f 0x4a7484aa 0x5cb0a9dc 0x76f988da
0x983e5152 0xa831c66d 0xb00327c8 0xbf597fc7 0xc6e00bf3 0xd5a79147 0x06ca6351 0x14292967
0x27b70a85 0x2e1b2138 0x4d2c6dfc 0x53380d13 0x650a7354 0x766a0abb 0x81c2c92e 0x92722c85
0xa2bfe8a1 0xa81a664b 0xc24b8b70 0xc76c51a3 0xd192e819 0xd6990624 0xf40e3585 0x106aa070
0x19a4c116 0x1e376c08 0x2748774c 0x34b0bcb5 0x391c0cb3 0x4ed8aa4a 0x5b9cca4f 0x682e6ff3
0x748f82ee 0x78a5636f 0x84c87814 0x8cc70208 0x90befffa 0xa4506ceb 0xbef9a3f7 0xc67178f2

SHA-256 is a 256-bit hash and is meant to provide 128 bits of security against collision attacks. SHA-512, in Chapter 3, is a 512-bit hash, and is meant to provide 256 bits of security against collision attacks. To obtain a 384-bit hash value (192-bits of security) will require truncating the SHA-512 output

SHA-256 operates in the manner of MD4, MD5, and SHA-1: The message to be hashed is first

1. Padded with its length in such a way that the result is a multiple of 512 bits long, and then
2. parsed into 512-bit message blocks M (1); M(2)::::M(N).

The message blocks are processed one at a time: Beginning with a xed initial hash value H (0), sequentially compute

H (i) = H(i 1) + CM(i) (H(i 1));

Where C is the SHA-256 compression function and + means word-wise mod 232 addition. H(N) is the hash of M.

Secure Hash Algorithm

A Cryptographic Hash is a kind of signature for a text or data file. SHA-256 generates a unique 256bit (32-byte) signature for a text. A hash is a one way cryptographic function and is a fixed size for any size of source text.

> The SHA-256 compression function operates on a 512-bit message block and a 256-bit intermediate hash value. It is essentially a 256-bit block cipher algorithm which encrypts the intermediate hash value using the message block as key. Hence there are two main components to describe:

(1) The SHA-256 compression function,

(2) The SHA-256 message schedule.

$\oplus$	bitwise XOR
$\wedge$	bitwise AND
$\vee$	bitwise OR
$\neg$	bitwise complement
$+$	mod 2^{32} addition
R^n	right shift by n bits
S^n	right rotation by n bits

The initial hash value $H^{(0)}$ is the following sequence of 32-bit words (which are obtained by taking the fractional parts of the square roots of the rest eight primes)
$H_1^{(0)}$ = 6a09e667
$H_2^{(0)}$ = bb67ae85
$H_3^{(0)}$ = 3c6ef372
$H_4^{(0)}$ = a54ff53a
$H_5^{(0)}$ = 510e527f
$H_6^{(0)}$ = 9b05688c
$H_7^{(0)}$ = 1f83d9ab
$H_8^{(0)}$ = 5be0cd19

Computation by preparing the message

1. Pad the message in the usual way: Suppose the length of the message M, in bits, is `. Append the bit \1" to the end of the message, and then k zero bits, where k is the smallest non-negative solution to the equation `+ 1 +k 448 mod 512. To this append the 64-bit block which is equal to the number ` written in binary. For example, the (8-bit ASCII) message \abc" has length 8 3 = 24 so it is padded with a one, then 448 (24 + 1) = 423 zero bits, and then its length to become the 512-bit padded message

$$01100001\ 01100010\ 01100011\ 1\ \underbrace{00\cdots0}_{423}\ \underbrace{00\cdots011000}_{64}.$$

The length of the padded message should now be a multiple of 512 bits.

2. Parse the message into N 512-bit blocks $M^{(1)}$; $M^{(2)}$; : : : ; $M^{(N)}$. The rest 32 bits of message block i are denoted $M_0^{(i)}$, the next 32 bits are $M_1^{(i)}$, and so on up to $M_{15}^{(i)}$. We use the big-endian convention throughout, so within each 32-bit word, the left-most bit is stored in the most sign can't bit position.

Definition:

Six logical functions are used in SHA-256. Each of these functions operates on 32-bit words and produces a 32-bit word as output. Each function is defined as follows:

$$Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z)$$
$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$
$$\Sigma_0(x) = S^2(x) \oplus S^{13}(x) \oplus S^{22}(x)$$
$$\Sigma_1(x) = S^6(x) \oplus S^{11}(x) \oplus S^{25}(x)$$
$$\sigma_0(x) = S^7(x) \oplus S^{18}(x) \oplus R^3(x)$$
$$\sigma_1(x) = S^{17}(x) \oplus S^{19}(x) \oplus R^{10}(x)$$

3. Experiments and results

3.1. **User registration**

User Registration is used to register the new user into the system and here he has to give his details like name, DOB, city etc. after the successful registration the user can login into the system.

3.2**Admin**

The Admin is a person who controls the entire ticketing system. The admin is used to enter the train details of the train like is adding new train information, deletion of trains, trail seat availability, train ticket fare for various seats, etc. the admin can restrict the particular passenger to use the system if any illegal activity found against him. The admin can change the train route also.

3. 3**Ticket Booking**

Ticket booking is used to book the train ticket. The passenger needs to select the source station and the destination station and he can select the particular train. Here the user needs to select desire seats like first ac, second ac, third ac, sleeper class; chair car, second seating and they can pay by different payment option like Internet banking, debit card, credit card, UPI method etc. Along with all the journey the passenger needs to give their details needed for the verification.

3.4 **Aadhar detail**

The Aadhar card is the unique 12 digit number given by the government of India to the individuals Aadhar details registration is very important module. Here the user needs to enter his complete details along with the Aadhar card number, and here we are assigning the finger print for the particular user.

3.5 **Verification**

Verification is used to verify the passengers during the TT verification. In this project here we will be uploading an image that will be further matched with the pre registered with the passengers Aadhar Card number.

3.6**E-MAIL**

Electronic mail (e-mail) is one of the most popular net-work services nowadays. Most e-mail systems that send mail over the Internet use simple mail transfer protocol (SMTP) to send messages from one server to another. The messages can then be retrieved with an e-mail client using either post office protocol (POP) or Internet message access protocol (IMAP). SMTP is also generally used to send messages from a mail client to a mail server in "host-based" (or Unix-based) mail systems, where a simple m-box utility might be on the same system [or via Network File System (NFS) provided by Novell] for access without POP or IMAP.

SMTP

SMTP is used as the common mechanism for transporting electronic mail among different hosts within the transmission control protocol/Internet protocol (TCP/IP) suite. It is an application layer protocol. Under SMTP, a client SMTP process opens a TCP connection to a server SMTP process on a remote host and attempts to send mail across the connection. The server SMTP listens for a TCP connection on a specific port (25), and the client SMTP process initiates a connection on that port (Cisco SMTP, 2005). When the TCP connection is successful, the two processes execute a simple request–response dialogue, defined by the SMTP protocol, in which the client process transmits the mail addresses of the originator and the recipient(s) for a message. When the server process accepts these mail addresses, the client process transmits the e-mail instant message. The message must contain a message header and message text ("body") formatted in accordance with RFC 822.

E-mail is used to send the e-mail in case of any illegal activities like during the verification if the finger print does not match or if anyone is trying to travelling illegally. The email will go to the railway department so that they can do further enquiry for the passenger.

5. REFERENCES

1. Multimodal Biometric authentication Combining Finger Vein and Finger Print Volume 7, Issue 10 (July 2013).
2. Fingerprint recognition using standardized fingerprint model IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010.
3. Adaptive Fingerprint Image Enhancement with Emphasis on Pre-processing of Data Issues 2, Vol.22 Year 2013.
4. A Study of Biometric Approach Using Fingerprint Recognition Vol. 1, Number 2, May 2013.
5. Fingerprint-Recognition-Using-Image-Segmentation-IJAEST-Vol-No-5-Issue-No-1-012-023
6. Chaos Image Encryption using Pixel shuffling-CSIT DOI:10.512/csit.2011.1217
7. Image Encryption based on diffusion and multiple chaotic Maps-IJNSA Vol. 3 No.2, March 2011.
8. Block based image encryption using Iterative Arnold transformations-IJARCSSE Vol.3 Issue 8, August 201
9. Image encryption base approach to address privacy and security issue in RFID Tags-IJCSMC Vol.4 Issue.5, May 2015
10. Image Encryption with RSA and RGB randomized Histograms-IJARCCE Vol.2 Issue 11, November 201.
11. A High Speed And Low Speed Image Encryption with 128-Bits AES Algorithm-IJCEE, Vol.4 No. 3, June 2012.
12. Development of an Online Bus Ticket reservation System for a Transportation Service in Nigeria-IISTE Vol.5, No. 12, 2014

13. Ticketing System of Indian railways through SMS and Swapping Machine-IJARCSSE Vol. 3 Issue 8, August 2013
14. An Evolution of the Operation of the railway E-Ticketing System. iBusiness,2012, June 2012
15. Fingerprint Based Identification System :A Survey – IJCTEE Vol.1 Issue 3

Author Profile

Yogesh Suman received the B. Tech degrees in Information Technology SRM University in 2017