The Smart Card Authentication System

Ms. Veena G[1], Ms. Jagadamba A

[1]Assistant Professor, Department of CSE, Vemana Institute of Technology

[2]Assistant Professor, Department of CSE, Vemana Institute of Technology

[1]veena_uin@yahoo.com, [2]jagadamba.reddy@gmail.com

Abstract

This paper provides details on smart card authentication software. The software uses the smart card, smart card reader/writer device, NFC (Near Field Communication), data card printer, and web application. The data collected from the user through the web application will be stored in the smart card in encrypted format using a smart card writer during registration and also basic details of the user will be printed on the smart card using the data card printer. When the user produces the card for authentication the smart card reader, reads and decrypts the details stored in the smart card.

Keywords: NFC, Data card printer, Encryption, Decryption, ACR122U, APDU.

Introduction

The verification of the identity of the user by the system is known as authentication [2]. The user should be fully authenticated, before authorization. Authentication tells whether the user can be allowed to enter into a particular system or not. Authorization tells once the user has entered into the system what parts of the system the user can access. The authorization will be based on roles associated with the user. The simplest way to authenticate the user is based on the user id and password mechanism. As password-based user authentication is prone to brute force attack [3], many user authentication mechanisms are implemented one such authentication mechanism is based on smart cards.

NFC [4] (Near Field Communication), is a type of technology that is based on radio frequency. NFC allows the exchange of information over a small distance (4 to 10 cm) among many electronic devices such as computers, tags, mobiles, etc. Advanced Card Systems Ltd. has designed **ACR122U NFC Reader**. ACR122U is a contactless smart card reader/writer which can be linked to a personal computer.

ACR122U [1] smart card reader is used to read and write data into the smart card. A smart card has a microchip that can store user information, 1K card has 16 sectors, and each of the 16 sectors consists of 4 consecutive blocks, i.e. sector 0x00h has blocks numbered 0x00h, 0x01h, 0x02h, and 0x03h, sector 0x0Ah has blocks numbered 0x28h, 0x29h, 0x2Ah, and 0x2Bh, etc. Each block can store 16 bytes of data. There are 48 blocks that can store data. There are 16 blocks that act as Trailer blocks. Data is stored only in Data blocks. Before reading or writing data into a smart card the data blocks need to be authenticated. The APDU (Application Protocol Data Unit) used for authentication is given in equation 1.

APDU = {FF 88 00 04 60 00h} ……….. Equation 1

APDU given in equation 1 authenticates the 4th block. If one block in a sector is authenticated, then there is no need to authenticate the other 3 blocks in that sector, and 88 indicates authenticate instruction.

APDU for reading data from a smart card is given in equation 2.

APDU = {FF B0 00 04 10h} ……….. Equation 2

APDU given in equation 2 reads data from the 4th block, B0 is the read instruction, and 10h in equation 2 indicates the number of bytes of data to be read.

APDU for updating or writing data into the smart card is given in equation 3.

APDU = {FF D6 00 04 10 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F} .. Equation 3

APDU given in equation 3 updates or writes data to the 4th block, D6 is the write instruction, and {00 01 .. 0Fh} is the data to write into the smart card 4th block.

The authentication application collects the user information from the user through a web application, collected data is stored in the database. During the time of the smart card issue, the data from the database is fetched for the corresponding user, and using authentication and write, APDU's the data will be written into the smart card. When the user produces the smart card for authentication, read APDU is used to read data from the smart card.

Literature Review

Data stored in the smart card can be read by any application if it is not encrypted. Encryption is the process of disguising the data into the cipher text so that unauthorized users will not be able to understand the cipher text. Decryption is the process of converting cipher text to original text. Encryption and decryption are part of cryptography, there are two types of cryptography symmetric-key cryptography and asymmetric-key cryptography. Symmetric key cryptography uses a single key for encryption and decryption. Asymmetric key cryptography uses a different key for encryption and decryption, but the keys are related to each other. Caesar cipher is one of the oldest ciphers, In Caesar cipher encryption [5], every letter is replaced by a letter that comes after the 'k' letters, in Caesar cipher decryption, every letter in the cipher text is replaced by a letter that comes 'k' letter before the cipher text letter. DES (Data Encryption Standard) [6], AES (Advanced Encryption Standard) [7], Blowfish [8], and RC4 [9] are a few examples of symmetric encryption algorithms.

RSA [10] is an asymmetric key cryptographic algorithm, which is based on prime factorization, it follows a one-way function or trap-door function [11]. In RSA given two large prime numbers, it is very easy to obtain a product of given numbers. But it is very difficult to get back the prime numbers given the product.

ECC [11] Elliptic Curve Cryptography is an asymmetric key algorithm. It follows a one-way function or trap door function [12]. For prime curve, over Z_p a cubic equation is used in which the variables and co-efficient all take on values in the set of integers 0 through p-1, and calculations are done using modulo p.

$$y^2(mod\ p) = (x^3 + ax + b) mod\ p \text{ …. Equation 4}$$

Consider the equation $Q = kP$ where $Q, P \ \in E_P(a, b)\ and\ k < P$. It is relatively easy to calculate Q given k and P, but it is hard to determine k given Q and P. This is called a discrete logarithm problem for elliptic curves. To prevent a brute force attack RSA algorithm requires a key of large size but the elliptic curve cryptography needs a key of smaller size.

Design and Implementation

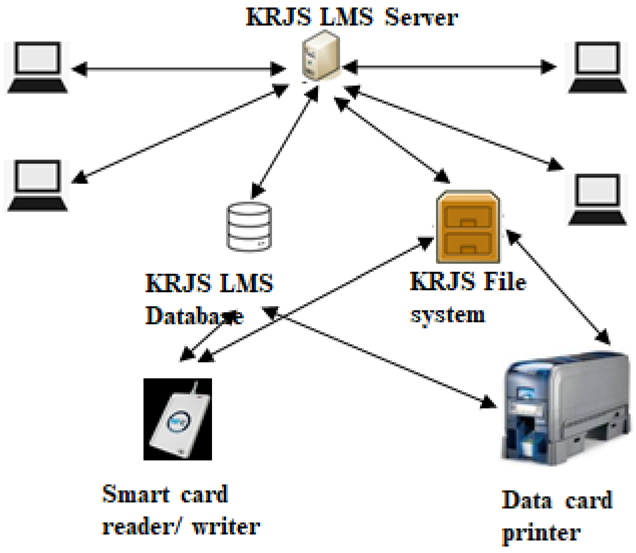


Fig 1. System Architecture

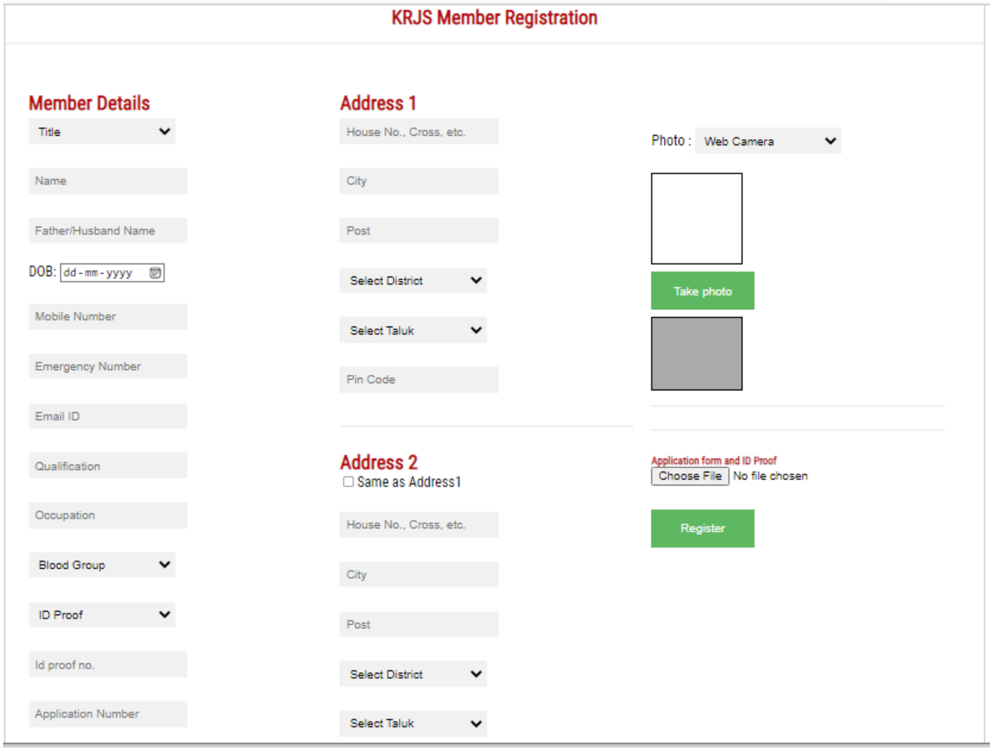
Fig 1. shows the architecture of the system. It follows client-server architecture; clients request data from the server through the HTTP/HTTPS protocol. The server prepares a response depending on the request by fetching data from a database or file system. The server sends a prepared response to the respective client. A standalone application is designed to interface the smartcard reader/ writer and data card printer.

During the time of member registration, the basic details of the member are stored in the database. While writing data into a smart card, the standalone application fetches the required data from the database and writes it into the data blocks of the smartcard. The size of the data that can be stored in the smart card is limited, hence instead of storing the data in key-value pair, the values are separated by a delimiter ^. In order to provide more security, the value is encrypted using RSA public key algorithm and the encrypted values are written to blocks of data card.

In the print module, the basic details of the user are fetched from the database, and the user photo from the file system of the server, details will be printed on the smart card using the data-card printer.

During the time of authentication, the smart card will be read by the standalone program. The data is decrypted using RSA public key algorithm. The decrypted data is tokenized using a delimiter. The data obtained after tokenization will be displayed, and the user will be authenticated.

Results



KRJS Member Registration

Member Details

Title
Name
Father/Husband Name
DOB: dd-mm-yyyy
Mobile Number
Emergency Number
Email ID
Qualification
Occupation
Blood Group
ID Proof
Id proof no.
Application Number

Address 1

House No., Cross, etc.
City
Post
Select District
Select Taluk
Pin Code

Address 2

☐ Same as Address1
House No., Cross, etc.
City
Post
Select District
Select Taluk

Photo : Web Camera

Take photo

Application form and ID Proof
Choose File No file chosen

Register

Fig 2. Member Registration form

Fig 2, shows the member registration form which collects the basic details of the member, address, and photo using a web camera.

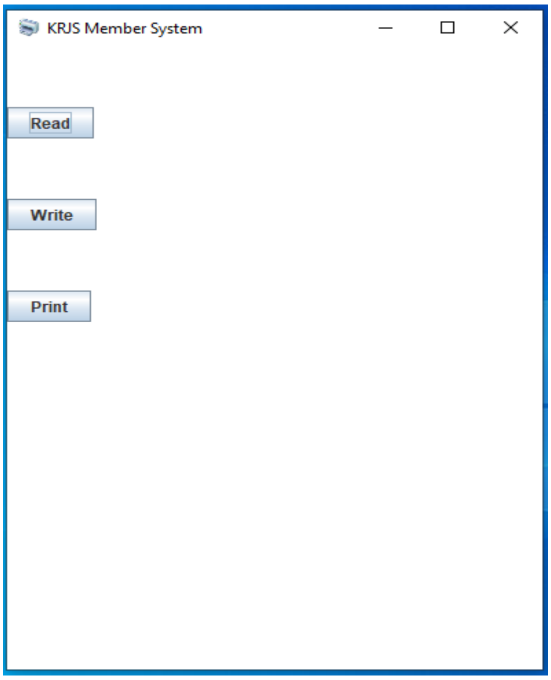
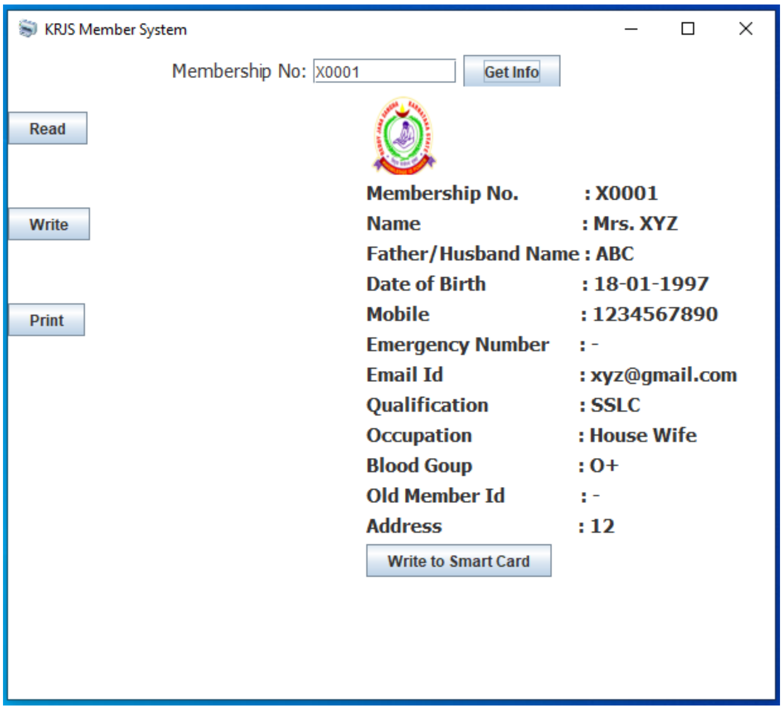


Fig 3. Smart card operations

Fig 3, shows the screen which has buttons for reading, writing and printing a smart card.

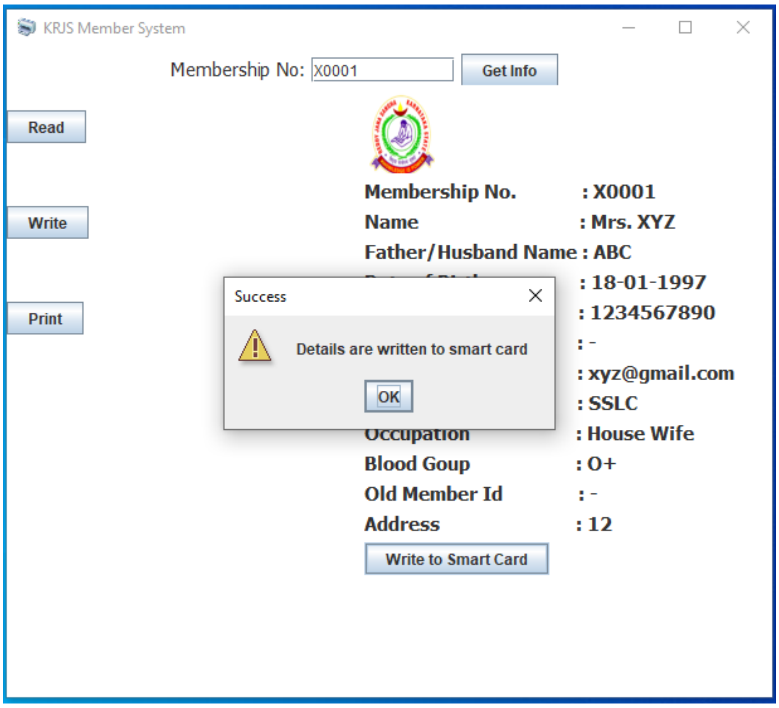


Membership No: X0001

Membership No. : X0001
Name : Mrs. XYZ
Father/Husband Name : ABC
Date of Birth : 18-01-1997
Mobile : 1234567890
Emergency Number : -
Email Id : xyz@gmail.com
Qualification : SSLC
Occupation : House Wife
Blood Goup : O+
Old Member Id : -
Address : 12

Fig 4. Data fetch

Fig 4, shows the screen which fetches details of member X0001 from the database to write into the smart card.



Membership No: X0001

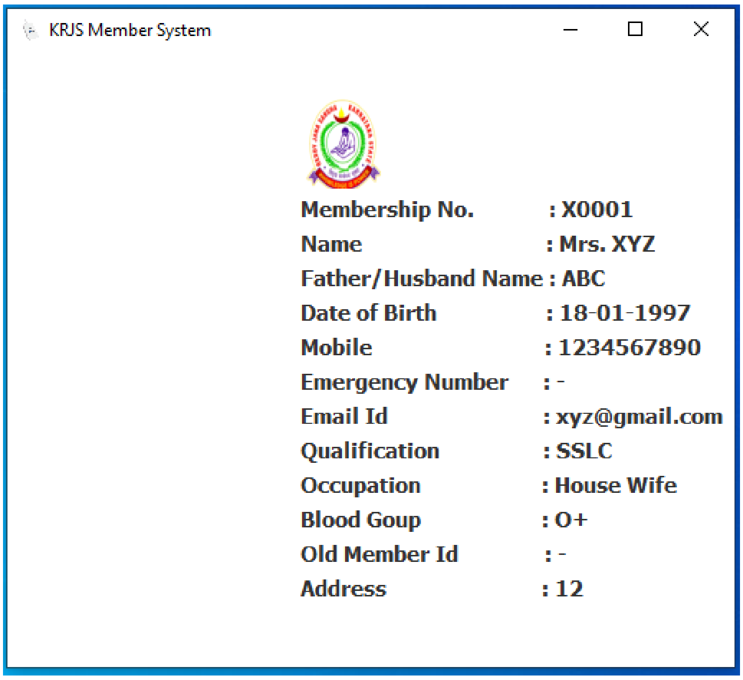
Membership No. : X0001
Name : Mrs. XYZ
Father/Husband Name : ABC
: 18-01-1997
: 1234567890
: -
: xyz@gmail.com
: SSLC
Occupation : House Wife
Blood Goup : O+
Old Member Id : -
Address : 12

Success

Details are written to smart card

Fig 5. Write data to smart card

Fig 5, shows the screen which writes data to smart card and shows confirmation message.



Membership No. : X0001
Name : Mrs. XYZ
Father/Husband Name : ABC
Date of Birth : 18-01-1997
Mobile : 1234567890
Emergency Number : -
Email Id : xyz@gmail.com
Qualification : SSLC
Occupation : House Wife
Blood Goup : O+
Old Member Id : -
Address : 12

Fig 6. Read data to smart card

Fig 6, shows the screen that contains data read automatically from smart card when the card is in the range of smart card reader device.

Conclusion and future enhancements

Users will be authenticated based on the smart card. During the time of user registration, the basic details of the user will be collected and stored in the database. The smart card writer a standalone application queries the database and writes required data into the data blocks of the smart card. When the user produces a smart card for authentication, the smart card reader a standalone application will read the data from the smart card and display it to the user. The application will be effective if biometric authentication is combined with smart card authentication, which is the future scope of this work.

References

[1] ACR122U USB NFC Reader, Application Programming Interface V2.02, http://downloads.acs.com.hk/drivers/en/API-ACR122U-2.02.pdf

[2] Ghizlane Moukhliss, Reda Filali Hilali, Hicham Belhadaoui, Mounir Rifi, “A New Smart Cards Based Model for Securing Services”, IJCSIS, Vol. 17, No. 1, January 2019, pp, 41-55.

[3] VarshaGrover, Dr. Gagandeep, “An Efficient Brute Force Attack Handling Techniques for Server Virtualization”, Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020

[4] Neeraj Kumar Singh, Near-field Communication (NFC) An Alternative to RFID in Libraries, Information Technology and Libraries, June 2020, https://doi.org/10.6017/ital.v39i2.11811

[5] Surabhi Aggarwal, “A review on enhancing Caesar cipher”, International Journal of Research Science & Management, June 2016.

[6] Kefa Rabah, “Theory and Implementation of Data Encryption Standard: A Review”, Information Technology Journal, 2005, pp-307-325

[7] Ako Muhammad Abdullah, “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data”, Cryptography and Network Security article, 2017.

[8] Ch. Usha Kumari, T. Pavani, A. Sampath Dakshina Murthy, B. Lakshmi Prasanna, M. Pala Prasad Reddy, “Generating Cipher Text using BLOWFISH Algorithm for Secured Data Communications”, IJITEE, 2019, pp-117-121

[9] Poonam Jindal, Brahmjit Singh, “A Survey on RC4 Stream Cipher”, ICICT-2014, pp-568-705

[10] Shireen Nisha, Mohammed Farik, “RSA Public Key Cryptography Algorithm – A Review”, International Journal of Scientific & Technology Research, pp-187-191.

[11] Sharad Kumar Verma, Badri Prakash Ojha, “A Discussion on Elliptic Curve Cryptography and Its Applications”, International Journal of Computer Science Issues, 2012, pp-74-77