# Smart Card for Healthcare System

Yogesh Kumar Sharma[1], Dr. S.Dixit[2]
[1]Research Scholar, [2]Professor
Deptt. of Computer Sc. & Engg., Mewar University, Chittorgarh (Rajasthan), INDIA

**Abstract:** Smart card is an embedded memory chip usually of pocket size which is compact and easy to carry. The growing multi professional health practice and explosion of healthcare data bring pose new challenges regarding access to data generated by different care givers in many care sites. The importance of integrating clinical data for effectiveness and efficiency of patient care and the need to safeguard privacy in an increasingly networked environment are the main challenges. Smart cards have the potentiality of solving these challenges. This paper aims to study the authentication of smart cards for the security of the patient records and a novel scheme has been suggestedwhich has a face recognition system for authentication. This will enable the access of information to the doctor during the case of emergencies, for a quick and quality assured care of the patient.

## Introduction

Smart card is a security token that has an embedded chip and contains encoded information within the microchip. The microchip on the smart card can either be a microcontroller or an embedded memory chip. Smart card can be made out of metal or plastic. The cards with a microcontroller chip have the ability to perform on-card proce0ssing functions and can add, delete and manipulate information in the chip's memory. Smart cards are designed to be tamper-resistant and use encryption to provide protection for in-memory information.

The first computer-on-a-chip was born in 1971 in Intel's laboratories. In 1974 Roland Moreno, a French independent inventor, mounted a chip on a card and devised a system to use the card for payment transactions. He showed his invention to a few French banks, and by the end of the year Honeywell Bull had produced the first CP8 Transac cards. The first mass use of smart cards was the Télécarte, a telephone card for payment in French pay phones which launched in 1983. As of 1995, Europe accounted for 342 of the estimated 484 million smart cards used worldwide. In the United States smart cards were used mainly for access control and corporate ID, but the number of these cards is negligible (well under 1 million).At the 1996 Olympic Games in Atlanta VISA launched a cash card, available in the disposable and reloadable versions. The card has a stored value of money and can be used for small purchases at participating merchants or more typically, at vending machines. The VISA Cash Card is also now available in Argentina, Australia, Canada, Colombia and Spain and a pilot project is currently being run in New York by VISA, MasterCard and Citibank.

Mohammad et al., [1] proposed four key characteristics of smart card which are portability, security, open platform and memory management. These four characteristics should be mainly considered while developing smart cards. K Eswar Kumar et al., [2] proposed a system to limit the access of the unauthorised person to high security locations based on access right of different persons. S Nivetha [3] has proposed two level authentications for smart cards. First level authentication is by using PIN, second level authentication is done by using SHA-256. Mohit Agarwal et al., [4] proposed a system for the user authentication using RFID Tag in smart cards. If the user is found authentic then the quantity of ration will be given to the customer according to the total number of family members displayed. C Lambirinoudakis et al.,[5] proposed a system to store medical based insurance information in smart cards. Smart card technology can be utilized for the implementation of securing the medical records carried by him/her. Alvin T Schan [6] this paper highlights the benefits of combining world wide web and smart card technology to support a mobile health management framework. Geylanikardas E et al., [7] they proposed a system by implementing the previous paper [6]. In this paper they have used smart card to provide access for the healthcare providers. Kuo-Hui Yeh et al., [8] Research paper on robustness of an E-healthcare system with smart card based authentication. Raul Sanchez-Reillo et al., [9] proposed a microprocessor smartcard with fingerprint user authentication. Vanga Odelu et al., [10] proposed a robust and efficient multi server authentication scheme using biometric based smart card and elliptic curve cryptography (ECC).

Smart cards are also being introduced for identification and entitlement by regional, national andinternational organizations. These cards are now-a-days extensively used for citizen cards, driving license and patient cards. Owing to the increasing growth of population in India, the medical facilities are become very limited. The health support system is far from ideal especially in rural India. The maintenance and sharing of digital health records securely is a significant challenge. We propose a novel scheme which has a two-step verification which consists of fingerprint and voice biometry.

**Proposed block diagram**

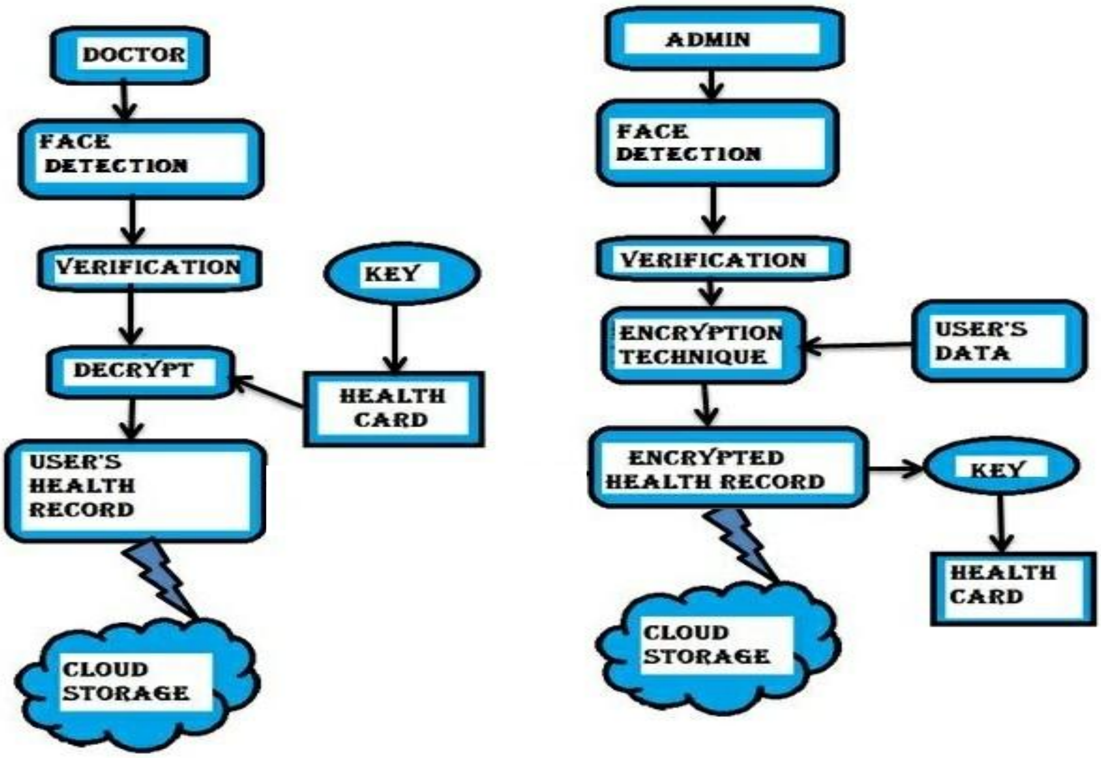


Fig. 1: General Block diagram of the proposed novel scheme.

**RFID Tags**

A radio-frequency identification system uses tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response.

RFID tags can be either passive, active or battery-assisted passive. An active tag has an on- board battery and periodically transmits its ID signal. A battery-assisted passive (BAP) has a small battery on board and is activated when in the presence of an RFID reader. A passive tag is cheaper and smaller because it has no battery; instead, the tag uses the radio energy transmitted by the reader. However, to operate a passive tag, it must be illuminated with a power level roughly a thousand times stronger than for signal transmission. That makes a difference in interference and in exposure to radiation.

Tags may either be read-only, having a factory-assigned serial number that is used as a key into a database, or may be read/write, where object-specific data can be written into the tag by the system user. Field programmable tags may be write-once, read-multiple; "blank" tags may be written with an electronic product code by the user.

RFID tags contain at least three parts: an integrated circuit for storing and processing information that modulates and demodulates a radio-frequency (RF) signals; a means of collecting DC power from the incident reader signal; and an antenna for receiving and transmitting the signal. The tag information is stored in a non-volatile memory. The RFID tag includes either fixed or programmable logic for processing the transmission and sensor data, respectively.

An RFID reader transmits an encoded radio signal to interrogate the tag. The RFID tag receives the message and then responds with its identification and other information. This may be only a unique tag serial number, or may be product-related information such as a stock number, lot or batch number, production date, or other specific information. Since tags have individual serial numbers, the RFID system design can discriminate among several tags that might be within the range of the RFID reader and read them simultaneously.

**Card Reader**

The term reader used to describe the hardware that interfaces with personal computers (PC) as a peripheral device for the majority of its processing requirements. Both readers and terminals read and write to smart cards. Smart cards can communicate singly or combinly. A Passive Reader Active Tag (PRAT) system has a passive reader which only receives radio signals from active tags (battery operated, transmit only). The reception range of a PRAT system reader can be adjusted from 1–2,000 feet (0–600 m)[citation needed], allowing flexibility in applications such as asset protection and supervision.

An **Active Reader Passive Tag (ARPT)** system has an active reader, which transmits interrogator signals and also receives authentication replies from passive tags.

An **Active Reader Active Tag (ARAT**) system uses active tags awoken with an interrogator signal from the active reader. A variation of this system could also use a Battery-Assisted Passive (BAP) tag which acts like a passive tag but has a small battery to power the tag's return reporting signal. Fixed readers are set up to create a specific interrogation zone which can be tightly controlled. This allows a highly defined reading area for when tags go in and out of the interrogation zone. Mobile readers may be hand-held or mounted on carts or vehicles.

**Encryption**

The encryption scheme used is AES symmetric encryption. The Advanced Encryption Standard, or AES, is a symmetric block cipher is used to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which the cipher transformations are repeated over a number of encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

The first transformation in the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows, the third mixes columns. The last transformation is a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key -- longer keys need more rounds to complete.

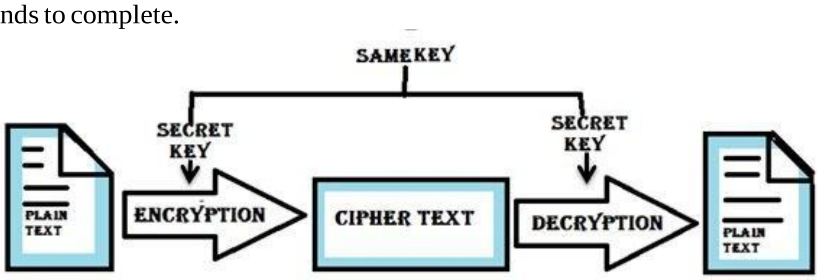


Fig. 2: General Block diagram of the advanced encryption scheme.

**Face API**

Face rectangle (left, top, width, and height) indicating the face location in the image is returned along with each detected face. Optionally, face detection extracts a series of face related attributes such as pose, gender, age, head pose, facial hair, and glasses. Face rectangle (left, top, width, and height) indicating the face location in the image is returned along with each detected face. Optionally, face detection extracts a series of face related attributes such as pose, gender, age, head pose, facial hair, and glasses.

Face recognition is widely used in many scenarios including security, natural user interface, image content analysis and management, mobile apps, and robotics. Four face recognition functions are provided: face verification, finding similar faces, face grouping, and person identification. Face API verification performs an authentication against two detected faces or authentication from one detected face to one person object.

**Cloud Storage**

Cloud storage is a model of data storage in which the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Here cloud storage is used for the secure storage of the patient medical health record.

Cloud storage is made up of many distributed resources, but still acts as one, either in a federated or cooperative storage cloud architecture

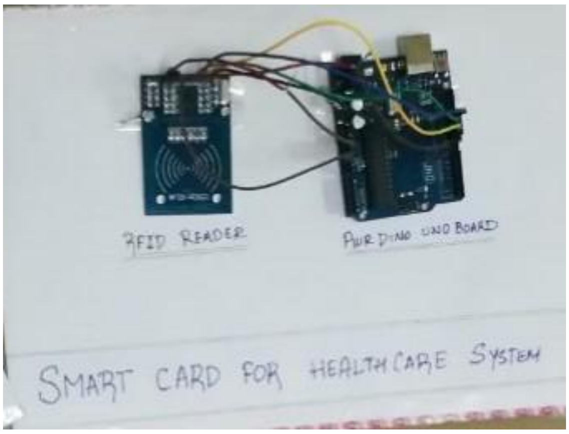
- Highly fault tolerant through redundancy and distribution of data
- Highly durable through the creation of versioned copies

The major applications of the proposed novel scheme can be found in the following domains:

- Improves patient identification.
- Improves medical record managements.
- Improves quality of care.
- Improves the security, confidentiality and privacy of the patient information.

- Quick access to the required medical information duringemergencies.
- Increases the hospital administrativeefficiency.

## Results and Future Implementations



1. Linking the Health card with AADHAR so that even if the health card is lost, doctor can access the healthcare data via AADHAR number of the patient.
2. Further improvement in the encryption of the health data can be done
3. Regular updation of the parameters such as Blood Pressure, Blood sugar can be done by linking this to smart health device.

## Conclusion

Smart card is typically a type of chip card that contains an embedded computer chip- either a memory or a microprocessor type that stores and transacts the data. Most of the countries lack integrated patient record system. Patients should fill the medical history forms each time they visit a new doctor. Eventually, over a period of time the medical records may get damaged and also can be difficult to access. If there are medical mistakes, it may take life of a person. This paper aims to get the best solution to the problems of handling and sharing of medical health records securely. This study is done extensively on the existing literature. More specifically, advancement in the smart card technology for healthcare systems. In our novel scheme, A smart card acts as a key to access the sensitive medical health record which is stored in the cloud. The doctor will be able to access the record once the system verifies him as a valid user through Face API System. The medical Health record will be safely stored in the cloud as we are using the Advanced Encryption Scheme for encrypting the medical health records. This makes the healthcare data more secure and easy to access whenever required as the smart card is compact and portable.

## Reference

[1] L. A Mohammed, Abdul Rahman Ramli, V. Prakash and Mohamed B. Daud, “Smart Card Technology: Past, Present, and Future,” International Journal of The Computer, the Internet and Management, Vol. 12, no. 1 PP. 12-22, Jan-April, 2004.

[2] K. Eswar Kumar1, Ashok Kumar Yadav2, Dr. T. Srinivasulu3, “Smart Card based Robust Security System,” International Journal of Engineering Inventions, Vol. 2, PP. 29-35, Issue 5, March 2013.

[3] S. Nivetha, “Secure authentication process in smart cards,” Conference: 2016 10th International Conference on Intelligent Systems and Control (ISCO), January 2016.

[4] Mohit Agarwal, Manish Sharma, Bhupendra Singh, Shantanu, “Smart ration card using RFID and GSM technique,” Confluence The Next Generation Information Technology Summit (Confluence), IEEE publisher, 5th International Conference 2014.

[5] C. Lambrinoudakis, S. Gritzalis, “Managing Medical and Insurance Information Through a Smart- Card-Based Information System,”

[6] Alvin T.SChan, “WWW + smart card: towards a mobile health care management system,” Journal of Medical Systems , VoL. 24, Issue 4, PP. 213–234, August 2000.

[7] GeylaniKardasE. TurhanTunali, “Design and implementation of a smart card based healthcare information system,”

[8] Kuo-Hui Yeh , N.W. Lo,Tzong-Chen Wu, “Analysis of an e-Health Care System with Smart Card Based Authentication,” Information Security (Asia JCIS), 2012 Seventh Asia Joint Conference , IEEE publisher, 13 September 2012.

[9] RaulSanchez-Reillo, L. Mengibar-Pozo and C. Sanchez- Avila, ”Microprocessor Smart Cards with Fingerprint User Authentication,” IEEE AESS Systems Magazine, March 2003.

[10] Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami, “A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards,” IEEE Transaction on information forensics and security, Vol. 10, no. 9, September2015.