Smart Card ID: An Evolving and Viable Technology

Praveen Kumar Singh[1], Research Scholar,
Department of Computer Application,
Shri Ramswaroop Memorial University,
Lucknow-Deva Road, India

Neeraj Kumar [2], Assistant Professor,
Department of CS & IT,
Babasaheb Bhimrao Ambedkar University (A Central University) Satellite Campus, Teekarmafil, Amethi, India

Bineet Kumar Gupta[3], Associate Professor
Department of Computer Application,
Shri Ramswaroop Memorial University,
Lucknow-Deva Road, India

***Abstract*—In today's world carrying a number of plastic smart cards to establish our identity has become an integral segment of our routine lives. Identity establishment necessitates a pre stored readily available data about self and to the administrator to authenticate it with claimer's personal information. There is a distinct requirement of a technological solution for nationwide multipurpose identity for any citizen across the board. Number of options has been exercised by various countries and every option has its own pros and cons. However, it has been observed that in most of the cases Smart Card solution has been preferred by a user and administrator both. The use of Smart cards are so prevalent that be it any profession, without incorporating its application, identity of any individual is hardly considered complete. In this paper, the principle aim is to discuss the viability of Smart Card technology as an identity solution and its ability to perform various functions with strong access control that increases the reliability of Smart Cards over other technologies. It outlines the overview of smart card technology along with its key applications. Security concerns of smart card have been discussed through an algorithm with the help of a division integer proposition. Possibilities of upgrading it with evolving technology offer it as a universal acceptability of identification. Capability of storing desired amount of information by an administrator to compute multiple operations to authenticate a citizen dictates its widening acceptability and an endeavor has been made in this paper to explain it through a proposed system flow chart.**

Keywords*—ISO; IoT; multipurpose; authentication; security; smart card reader; cryptography; identification technology; smart card application

I. Introduction

One takes today a burden of carrying a wallet with full of cards to establish his/her identity like official ID card, canteen cards, library cards, driving license, etc. Smart card ID has a potential to replace all these cards by a single smart ID cards to serve the desired purpose. Varieties of smart cards are available as on date with progressive technologies where developers use different data structures and standards for programming. In this paper, we will discuss about viability of smart cards as a solution to requirement of nationwide multipurpose smart ID for each and every citizen with continuous evolving technology. Our aim is to propose a viable technological solution for a single multipurpose smart ID card to do away with carrying multiple cards by an individual. It will assist governments across the globe in better administration with cost effective solution for multiple application single smart ID cards. It will also need management of a large database with processing and scalable computing to home on desired ID. Data centers handling these big data are contributing in reducing the delay and costs in data processing and improving the quality of service to include certain discrete services using internet based services. A smart card is an electronic device with micro-processor based system containing embedded integrated circuits which can process and store a large chunk of data and applications [4]. A smart card reader is used to access the stored information and it is also called smart called terminal when a card is plugged into this reader. Apart from the card reader, radio frequencies are also used to operate a smart card. Different protocols are being used for different types of card readers to communicate between card and the reader.

The standard of security adopted in the smart cards defines the degree of protection about sensitivity and confidentiality of data against the breaches. The issue with smart cards is its data storage capacity and processing capability. If we choose to associate any new application with smart card then the security mechanism would require consume more space which in turn necessitates use of lightweight security algorithm. In this paper a hypothetical case of a division integer algorithm is taken and then a viable system has been proposed to ensure appropriate security measures and to combat epidemics of cyber-crimes. In this respect, all the states need stringent legislations with effective law enforcement to prevent any frauds [5]. The objective of this paper is to touch upon smart card technology and its viability as single ID alternative with desired identity standards by various states and to study its viability with feasible applications.

II. Background

In order to drive any evolution, necessity propels an environment conducive to that particular commodity. The genesis of smart cards during later half of 1980's decade too in Europe was no exception. It was not security rather needs to do away with handling of large amount of cash which become the prime reason behind its evolution. The government of France used it as a technological solution against secure financial transactions. However, varying nature of issues cropped up including fraudulent production and failure of transactions in establishing identities of those initial smart card holders which were quite primitive in nature. It drove the manufacturers to introduce the cryptographic session between the control terminals and smart cards. Possibility of any skimming of smart cards could be ruled out due to their non-visibility by anyone from outside and no clone of any smart chips could be generated. It had a positive impact on transaction time and it was more cost effective too. In 1990's when magnetic stripes were replaced by microchips, the huge investment with support infrastructure by telecom companies in US brought revolutionary changes in smart cards. In those years, offline authentication continued to happen in Europe and with newer applications, they still dominate the smart card industry [1]. In contrast, US had no trouble with respect to overhead costs due to non-committal of desired level of authentication and having no bandwidth limitations.

During initial years, smart cards were used mainly in telephonic and health sectors. Those cards were utilized as memory cards and their implementation in 1990's as e-purse was no less than a revolution. Subsequently, US and Europe both adopted secure microcontroller smart cards against all financial transactions with debit/credit cards. 9/11 tragedy forced the world to have a relook in identity issues against terrorism and illegal immigration which boosted the required changes and resulted evolution in smartcards. With continuous evolution, smart cards now offer an excellent opportunity to various governments worldwide to implement e-governance applications [2], [3]. Utility of smart cards range from different applications, such as public usages like driving license, e-passports, etc. to private usages as cashless payment system like e-purse, access cards for identity verifications, etc.

III. Smart Card: An Overview

A smart card is known as a portable device which can compute, store and carry the data in an embedded processor chip for verification of personal identity in a secure repository. A smart card can also store a data in relation to any individual in the form of a barcode which are extracted through an optical scanner. Barcode is a representation of data displayed in a stripe of alternate black and white lines which is machine readable optically illustration of an object that carries it. Barcodes are depicted in a smart card by parallel lines with varied spacing's and widths. The initial smart cards were contact based while the contactless smart cards came in the early 90s. Later, smart card with contactless ICs completely revolutionized the smart card applications and its utility.

The contactless smart cards offer a high order of comfort to a user whereas it can be read without any physical contacts with bar code readers. It also extends an advantage over contact smart cards in terms of costs, durability and reliability [6]. An easy carriage of such smart cards in a wallet offers a good convenience to the users. A dedicated and secure transmission protocol is employed in a contactless smart card which offers it an excellent security. A magnetic tape is attached in the form of a stripe in the magnetic stripe smart cards. Memory smart cards are having a peculiar feature of storing and carry information which may be personal, financial or any other specific information. An embedded circuitry of IC on a card is referred as microprocessor smart cards which can process and store the subject data [7].

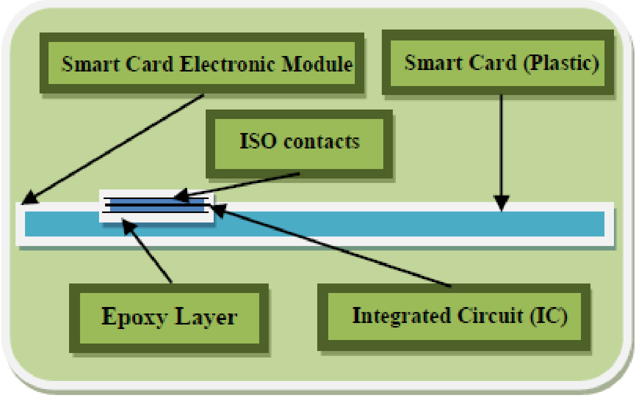

Fig. 1. Sideway structural view of a plastic smart card.

A sideway structural view of a plastic smart card is illustrated in Fig. 1 above. In order to protect the smart card chip from bends, it is generally placed on one of the edges of the smart cards. An Epoxy layer on this magnetic stripe is also visible when we take a view of its internal structure. Various applications, communication protocols and manufacturing specifications are defined by International Standardization Organization (ISO). Currently, there are following ISO standards for smart cards:

A. *Physical Characteristics:* Initial ISO standard (ISO 7816-1) in 1987 defined the card size of a smart card as 0.76 mm thick, 53.98 mm height and 85.6 mm wide. It has again been revised in 1998.

B. *Electronic Contacts:* ISO standard (ISO 7816-2) defined the size and location of the electronic contacts in smart cards. This too has been revised in 1998.

C. *Electrical Signals:* ISO standard (ISO 7816-3) defined transmission protocol along with the nature of electrical signals in smart cards. It has been thrice in 1992, 1994 and 1998.

D. *Communication Protocols:* ISO standard (ISO 7816-4) defined the communication protocols in different types of applications and file structure to be stored in these applications in smart cards. It has been revised twice in 1995 and 1998.

E. *Language:* ISO standard (ISO 7816-7) defined the commands of query language used in smart cards. This has been revised again in 1998.

The use of internet technology has changed the whole perception of security systems. Smart card technology too is not an exception. Identification of an individual is to do more with secure authentication rather secure identification. Individual credentials are required to be stored in a secured manner for which a portable smart card provides a good platform. The transactions made through the magnetic stripe of smart cards are processed by an electronic connection between the smart card and the service provider. Processor and memory chip in a smart card allows storing of required data which are processed by a smart card reader when connected through a centralized database [8]. Unlike the contact smart cards in which they have electrical contacts with a card reader, contactless smart cards operate through a transmission frequency and an internal antenna coil. It can be picked up and read through the external aerial.

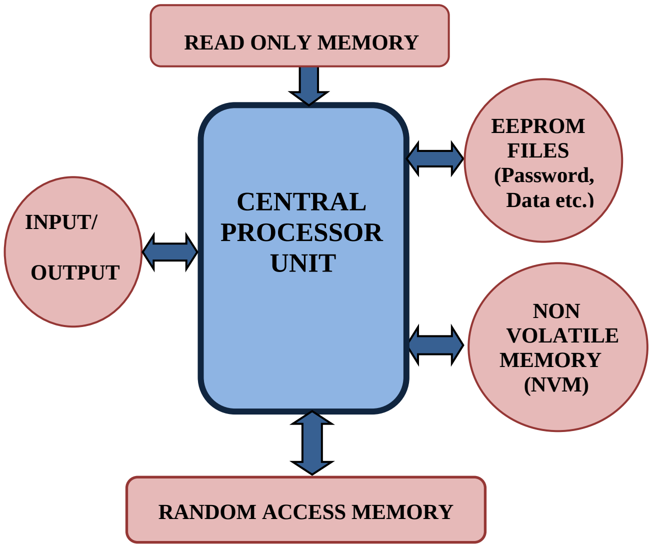

Fig. 2. Basic architecture of an electronic module of smart card.

TABLE I. Process Enabled Verses Memory Smart Card

Smart Card Features	**Types of Smart Cards**	
	Processor Enabled Smart Cards	***Memory Smart Cards***
Interfaces with Contact/Contactless Cards	Contact/Contactless/Both	Contact/Contactless/Both
Read Only Memory	YES	YES
Random Access Memory	YES	NO
Secure with Certified Data	YES	NO
Microprocessor	YES	NO
Example	Multi-Application Cards	Phone Card

The two most common materials utilized for manufacturing of smart cards are Acrylonitrile Butadiene Styrene (ABS) and Polyvinyl Chloride (PVC). There are two main categorizations of smart cards, namely, as processor enabled and memory smart cards. A relative comparison based on the various features between the two is shown above in Table I. Out of these two, memory smart cards are considered as basic smart cards with limited data storage capability with a nonvolatile memory features. These cards are transmitting data in only one direction and also termed as asynchronous smart cards and they are used offline only. On the other hand, processor enabled cards are using semiconductor technology and being a sophisticated cards they are also called as 'true smart cards'. These cards have smart chip which operates cryptographic functions and encryption technology to process secure data transmission [9]. In general, biometric technology is used to establish the identity of the user. These cards have bi-directional data transmission, possess significant memory and they are also termed as 'synchronous smart cards' and difficult to be duplicated. Data storage in such smart cards is nonvolatile and stored in EEPROM.

An electronic module of a smart card apart from an input/output component consists of different types of memories which include Read Only Memory (ROM), A (Random Access Memory), an electronically erasable Memory (EEPROM) and a non-volatile memory (NVM) as illustrated in Fig. 2 above. It is placed in the second layer of embedded processor chip of smart card as illustrated in the Fig. 1. These memory chips are incorporated in such electronic modules based on the projected requirement and at the same time presence of all memory chips is not sacrosanct. Bringing all these memories in a single integrated chip together not only reduces the size significantly, combining it with cryptography technology it also increases the security of smart card [10].

IV. Security Concerns in Smart Card ID

The primary function of a multipurpose smart card ID is to establish the identity of the user. One way of establishing an identity of an individual is to recognize him or her by verbal or visual means. For verification of facts with respect to the individual encryption technologies are being used. With number of transactional applications are being prevalent in smart cards, use of PIN is the most common methodology to establish the identity for any user. However, the constraint is to remember the number of PINs for different applications for any user. Therefore, to overcome this binding, biometric technology for verification of identity of an individual was introduced [11]-[13].

Biometric technology measures individual personal features. Presently, there are various kinds of biometric technologies are being used like signature, Retinal, palm geometry, fingerprints, recognition of facials and voice signatures, etc. Table II below indicates a comparison amongst the different types of biometric technologies. It offers a relatively fair comparison on different parameters like rate of acceptance, rate of rejections and comparative costs, etc.

There are better security provisions in smart cards than the normal printed/magnetic stripe identity cards. The primary motive of this security is to offer an authenticated access control or establishing guaranteed identity before any financial transactions to all the users of Smart cards [14]. As the security infrastructure is handled by human therefore, attacks of malicious users or hackers cannot be ruled out. There are various kinds of provisions which are prevalent to address the security concerns which include like micro-printing, holograms, optically variable printing in the memory technologies of smart cards. While employing security system in a smart card, the basic principles of security remains same as Privacy, Non-repudiation, Authentication, Integrity and Verification [15], [16].

Various types of encryption algorithms are being used in security systems of smart cards. These security mechanisms require a robust key management with a well-defined procedures and strong policy in place. A widely used public key infrastructure (PKI) security mechanism for data encryption ensures secure data exchange and confidentiality in most of these security systems. In order to establish authentication in security provisions like digital certificates or digital signatures, the encryption algorithms have a key role to play. Smart cards too make use of different encryption algorithms to implement the basic security principles [17]-[19].

TABLE II. A COMPARATIVE TABLE FOR SOME COMMON BIOMETRIC IDENTIFICATION (SOURCE: THE IBM SMART CARD DEVELOPMENT GROUP)

Methodology	***Rate of Acceptance***	***Rate of Rejection***	***File Size in Bytes***	***Relative Cost of Device***
Static Signature	20-90%	5%	1000-2000	Cheap
Dynamic Signature	20-70%	1-20%	40-1000	Medium
Hand Pattern	0-90%	5%	10-30	Medium to Expensive
Retinal Pattern	0-10%	1%	80-1000	Very Expensive
Fingerprint	0-100%	1-10%	300-800	Medium to Expensive
Voice Pattern	100%	10%	100-1000	Cheap
PIN	50%	1%	1-8	Very cheap

Let us take an example of a mathematical algorithm to be used for encryption of a message to be exchanged. A message is considered encrypted, if the information associated with the message can be veiled with some coding and it cannot be decipher by anyone until it is unveiled through decoding. The encrypted message is called crypto text while the normal message is called plaintext. In order to encrypt a message, one requires a key for coding which can be decrypted only if a receiver has same set of keys for decoding. For different individuals, different keys shall be required. Security of the key is of paramount importance against keeping confidentiality of information. As loosing either an encrypting or decrypting key to ant eavesdropper can lead to compromise the entire message.

If the keys used for encrypting or decrypted the message is same then the procedure is called 'Symmetric', however if the keys are different then it is called 'Non symmetric'. Usually, if one of the keys is available in public domain then the procedure is called 'public-key cryptography'. Symmetric encryption is also referred as 'cryptosystem' if it is in the form of a quintet (F, T, R, E, D), where R is a finite key, F is the finite 'message' (plaintexts) and T is a finite 'crypto text'. If for each key $r \in R$ the $e_r \in E$ stands for an 'encrypting function' and $d_r \in D$ stands for each 'decrypting function' whereas E is an 'encrypting function' which incorporates all achievable encrypting function. At the same time, D is referred as 'decrypting function' which incorporates all achievable decrypting function.

It signifies, $d_r(e_r(w)) = w$; where, w denotes the block message and r is referred to encrypting key.

A same message can be encrypted into different crypto texts by an encrypting function while encryption can be random and not a mathematical function. Mostly, all common encryption procedures are used either on number theory or on algebraic functions.

Let us take an example of "long division" Newton's method with a large base number in which M represents the dividend length whereas $O(M^2)$ indicates the basic operations. This method is quite efficient in which, m and n indicate divisor and dividend respectively. If we, assume M>N where M refers to length of a dividend and N refers to length of divisor, we find the result as m = qn + r in which q denotes quotient whereas r denotes remainder.

If DIV (m,n) = (q,r), then $q = \lfloor m/n \rfloor$.

Now, let us commence through the results of the divisor's inverse to obtain root of a function.

$$f(y) = n - 1/x, \text{ i.e. } 1/n, \qquad (1)$$

If, we use the Newton iteration

$$yi+1 = y_i - \{F(yi_i) / F'(yi_i)\} = 2\, yi_I - n\ yi_i^2$$

and compute $l = 10^N/n$, which indicates $g(y) = n - 10^N/y$ for a root of given function in which we achieve the accurate Newton iteration.

$$yi+1 = 2\, yi - (m\, yi^2 / 10^N) = 2\, yi - (yi^2 / L) \qquad (2)$$

In order to stay solely on integers, we may utilize an account of this iteration which becomes proximity to integers:

$$x_{i+1} = 2\, x_i - \lfloor (n / 10^N) \lfloor (x_i^2 / 10^{M-N}) \rfloor \rfloor$$

In a decimal arrangement, divisions through powers of 10 become insignificant. The aim of doing it is to determine $\lfloor L \rfloor$, with the floor $\lfloor m10^{-M} \lfloor L \rfloor \rfloor$ we find the required result and finally obtain the remainder. The properties which may be validated are expressed as:

$2x - \lfloor n10^{-N} \lfloor x^2 10^{N-M} \rfloor \rfloor \geq 2x - x^2/L$, it also signifies that iterants values are not reduced by rounding the integers.

At the same time, if $y \neq L$ then $2y - y^2/l < L$. Because $m/10^N < 1$,

We, therefore, find following corresponding value for rounded iteration from (2):

$$x_{i+1} = 2\, x - \lfloor (n / 10^N) \lfloor (x^2 / 10^{M-N}) \rfloor \rfloor$$

$$\leq 2\, x - \lfloor (n / 10^N) \{ (x^2 / 10^{M-N}) - 1 \} \rfloor$$

$$\leq 2\, x - \lfloor (x^2 / L) - 1 \rfloor < 2\, x - \lfloor (x^2 / L) - 1 \rfloor$$

$$\leq 1 + 2 \qquad (3)$$

If x < 1 then $2y - y^2/1 > y$; therefore the precise iteration grows till iterants become < 1 and the same phenomenon is applicable to a rounded iteration as well.

$$\text{When, we express } L = x_i + €_I \qquad (4)$$

In which $€_i$ represents an error. In Newton's methods for each correct number as per (3), amount compounds to double with each step and the same is applicable here as if xi < L.

$$|€_i| = l - y_i \leq l - 2y_{i-1} + (y_{i-1}^2 / L) = (€^2_{i-1} / L)$$

$$|\text{€}_i| \leq (\text{€}^2_{i-1} / L) \leq (1/L) (\text{€}^2_{i-2} / L)^2$$

$$\leq \ldots\ldots \leq L^{-(1+2+2^2+\ldots\ldots+2^{i-1})} \text{€}^{2i}_0$$

$$= L^{(1-2^i)} \text{€}^{2i}_0 < 10^{(1-2^i)(N-M)} \text{€}^{2i}_0$$

In this case, it is deed that $10^{(1-2^i)(N-M)} \text{€}^{2i}_0 \leq 1$.

Suppose that $|\text{€}_0| < 10^{(N-M)}$ which amounts to

$$i \geq \log_2 \lceil (N–M) / (N - M - \log_{10[\text{€}0]}) \rceil$$

Therefore, we find,

$$x_0 = 10^{M-N} \lfloor (10^N / n) \rfloor \quad \text{or}$$

$$x_0 = 10^{M-N} \lceil (10^N / n) \rceil$$

It all depends upon that which is closure to $10^N /n$, when $|\text{€}_0| \leq 10^{M-N}/2$, it then finds

$$I = \log_2 \lceil (N–M) / (\log_{10} 2) \rceil$$

$$= \lceil \log_2(N-M) – \log_2 (\log_{10}2) \rceil \qquad (5)$$

Akin to the iterations numbers, a set of growing sequence of integers is produced by using rounded integers with iteration till we find a value within [L, L + 2). Thereafter, we may check if it is the preceding correct value $\lfloor L \rfloor$ or the obtained value only. The entire procedure is as follows (output becomes DIV (m,n)):

Applicability of Newton's method: Division

We return (0, 0) and leave, if m = 0, we return (m, 0) and leave if n = 1 and with the corresponding value of equation (1), we return (–p, q) and leave, if n < 0, we find DIV (m, – n) = (p,q)

We return (– p –1, n – q), if q > 0 or (– p,0), if q = 0 and leave, if m<0, we find DIV(– m,n) = (p,q)

Length of divisor n → length of dividend m

and N→ Set M

We return (0,m) and leave, if M < N,

We return (p, m – np) and leave, if M = N , since $0 \leq p \leq 9$ (By trial), we easily find the quotient p

We find $\lfloor 10^N /n \rfloor$, if M > N, since $1 \leq \lfloor 10^N/n \rfloor \leq 10$ (By trial) And we set $10^{M-N}\lfloor 10^N /n \rfloor \rightarrow y_0$, or else we set $10^{M-N} (\lfloor 10^N /n \rfloor + 1) \rightarrow y_0$, if $10^N /m - \lfloor 10^N /n \rfloor \leq 1/2$ i.e.

$2 \text{ x } 10^N – 2n\lfloor 10^N /n \rfloor \leq n$, It is conditional with rider that at least one iteration has to be performed, if $y_0 > l$

The recursion will be

$$x_{i+1} = 2 x_i \lfloor (n / 10^N) \lfloor (x_i / 10^{M-N}) \rfloor$$

It will commence from x_0 till $i \geq 1$ and $x_{i+1} \leq x_i$.

It is checked through multiplications that either of the findings of x_i, $x_i - 1, \ldots$ is right $\lfloor l \rfloor$ and $\lfloor l \rfloor \rightarrow$ set q

$mp/10^M \rfloor \rightarrow$We set t (a multiplication) and verified by multiplications only as to which value t or t +1 is the right quotient p in division DIV(m, n) = (p, q). We find (p, m - np) and then we may leave.

$$p = (m – q) / n \leq n / m < (10^M /n) \qquad (6)$$

The accurate quotient is produced as #12 because firstly q < n and then further, if $\text{DIV}(10^M , n) = (k, q')$ then $q' < n$ and

$$mk / 10^M = (pn+q') (10^M – q) / n10^M$$

$$= p – (p q' / 10^M) + q \{ (10^M – q') / n 10^M \} \qquad (7)$$

On the right side of middle term in a interval is (−1, 0] and the last term becomes [0, 1). Therefore, p is having a value of either t+1 or t.

Since the iterations become very small due to the maximum number of 1 for the length M with the algorithm difference of the dividend and for the length N of the divisor whereas there are always at least three multiplications with an iteration step as described in 6 and 7and for a maximum of length 2N, there will be at least one subtraction for integers (some will remain constant). That is just an example of a division algorithm that is how it ensures security of information exchanged between two users.

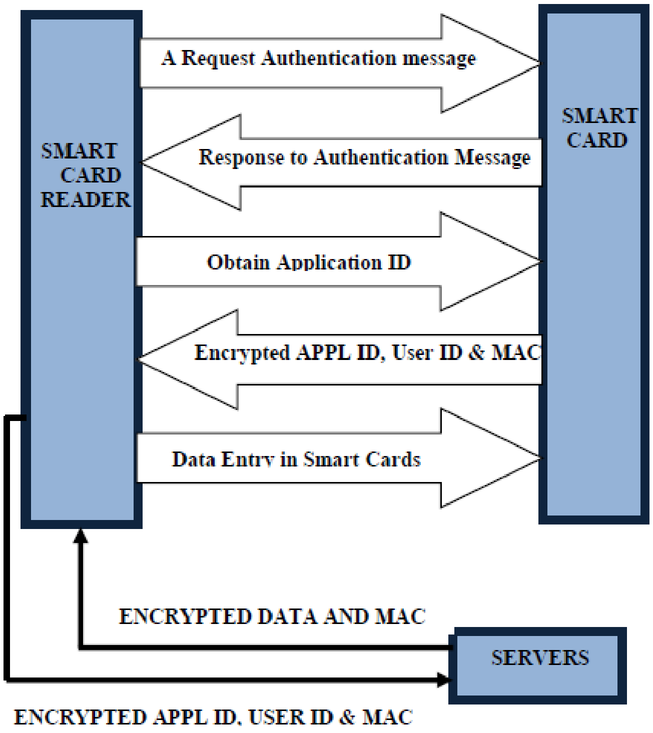
A Request Authentication message
Response to Authentication Message
Obtain Application ID
Encrypted APPL ID, User ID & MAC
Data Entry in Smart Cards
SMART CARD READER
SMART CARD
ENCRYPTED DATA AND MAC
SERVERS
ENCRYPTED APPL ID, USER ID & MAC

Fig. 3. Authentication process in smart card.

Let us also examine another cryptography technique of an authenticated encryption. This technique is used to ensure integrity and confidentiality of data. A Message Authentication Code (MAC) is combined with this and a symmetric encryption algorithm is used in this technique. In order to see how a smart card uses the symmetric encryption, we need to go through the mutual authentication process between a smart card and a smart card reader [20]. This authentication process requires a source of data which is provided by a server which holds a data structure for number of users.

The above mentioned flow amongst the server, a smart card and a smart card reader explains the authentication process in Fig. 3. In this process, the moment a smart card comes in contact with a card reader, an initial request of authentication is processed by smart card reader. Once the response from smart card is received by the card reader, an application ID is issued by smart card reader. It is responded by smart card with a user ID and a message authenticated code which is followed by an encrypted data feeding to smart card by the card reader [21], [22]. Meanwhile, the card reader is also attached to a server which responds with the user ID and an application ID along with a message authenticated code which precisely describes the authentication process in a smart card.

User trust is an important factor for success of any security system. Security measures used in a smart card needs to ensure of prevention of loss of data due to any human error or ill intent. Presently, encryption technology with computers is widely used for transmission or exchange of information. Ciphers were the most common methods to ensure security of data. Since, the complex security algorithms like DES, AES and many others are associated with data, probability of any direct attack is very minimal in various data transmission associated technologies including smart card security systems. However, a side channels attack on software and hardware systems of smart card cannot be ruled out. A malware to capture the key mechanism of security system may be employed by an attacker. Likewise, use of spy camera and other hardware technology to breach the security system of smart card to track the human implementation of encryption technology too warrants a high degree of caution while implementing the smart card technology [23].

V. Smart Card Applications

The major advantage of a smart card over a normal ID card is its capacity to store larger amount of information and its programmability for various applications. Its feature of having a possibility through contactless readers gives it an edge over similar technologies in pursuits of finding a nationwide single ID for multiple usages. The term ‘smart, relates with a particular type of application like memory/magnetic stripe/optical/microprocessor cards. The larger application of smart cards is its utility in financial transactions with faster processing of revenues or payments [24]-[27]. Its capability to carry the related information of an individual and to deliver it at desired destination distinguishes it from other such applications in identifying the veracity of the individual.

Smart card applications include its use as GSM mobile phone for the identity requirements. It’s wider use as a banking card in the form of debit/credit cards or being a tamper-proof/counterfeit device increase its popularity. Electronic coupons and credit programs are other attractive applications of smart cards [28]. The inherent security and flexibility of smart cards increases its utility. With improved data storage and security supplemented with provisioning of encryption and decryption by a user offers high rate of convenience to users. Some notable applications of smart cards are as:

A. *ID Validation*: The basic premise of storing the individual information is to verify him/her for any further uses in smart cards. Currently. A large number of organizations and institutions including government and private both are using smart card to extend access control to their members/employees only after due verification of their ID based on their personal information stored in their smart ID cards. It’s viability as an option for secure ID credential verification makes it a lucrative tool to be adopted by every potential organization.

B. *Data Authentication*: Information with respect to the user is authenticated by the data already stored in the smart card or a token system also known as knowledge arrangement based may be exercised for the purpose [29]. Token systems are generally employed in applications like passport verifications; credit cards, driving license, etc. whereas knowledge based authentications are exercised in applications with tokens system like PIN numbers.

C. *Financial Transactions*: Smart cards are very handy as a tool for financial transactions both in traditional and web based applications. A cash value can be stored in smart cards to use it as credit cards. It’s potential to support both consumers and business against lower rate of transactions widens its applicability in marketing targeted programs in financial services.

D. *Telecom Sector*: Provisioning of secure cellular communication is assisted by smart cards. New apps and functions are providing real time download capabilities by smart cards [30], [31]. A SIM card given by cellular operators to their subscribers and its use of multimedia applications like pay TV cards are making a very productive tool amongst normal public.

E. *Loyalty Marketing Programs*: A huge number of loyalty programs are being run by smart cards based applications by various business houses in services like retail shopping, telecommunications, air travel, etc. in which customers are being offered very attractive discounts. Such applications not only make business market very competitive, it also helps to normal public to receive benefits at relatively lower rates.

F. *Secure Computer Networks*: A secure access for networks can be assured through digital signatures of a user. They are utilized in granting only specified people to have the access to a particular computer network [32]. This mechanism is very handy and vital for the security related organizations. Encryption technology is making today computer networks more secure than the erstwhile networks.

G. *Healthcare*: Professionals from healthcare services are using smart card based applications to gain access for continuous updating of their data and its processing. A colossal amount of information is being shared in the form of drug prescription, physician details, dosage, etc. by these professionals. Patients use smart cards to provide their pre stored medical history with doctors and in making payments of their medical treatments as well.

H. *Other Smart Card Applications*: Its flexibility and potential to have repository of information supports it in vast number of applications. With secured online transactions in many commercial activities augurs well for both the service provider and subscribers. A wide range of services which are exploiting the smart card based applications include agricultural products, Life Insurance sector, vending machines, libraries, restaurants, laundry services, set top box facilities, software based games for kids, electronic toll collection, information technology, mass transit, parking facilities, e-passports etc. are just the few names to be counted [33]. Utility services like payment transaction, call counters, memory storage etc. employ smart card based applications.

Earlier, the smart cards were used as a memory card or PC cards. However, latest ones are having a smaller size, lighter weights, better storage capacity with lesser power needs are able to influence a wider chunk of applications By using the radio frequency with inbuilt antenna embedded in the smart card, it enables data transmission without any physical contact with the card reader from a distant terminals. Pre fielded bio-metric data about the user like, fingerprints, retina/iris scan; DNA pattern etc. increases its credibility in user's authentication. Smart cards do possess ability to assist in garnering demographic data for exercising the franchise by the voter. Industry association of smart cards has reported about use of billions of smart cards in healthcare, family planning, individual IDs and in many other applications [34]. The factors like privacy, economy, legal and technological issues require a continuous address due to its widespread usage. Worldwide, travelers are using it as an international traveler check which is facilitated by secured transactions.

VI. Research Approach

On one hand, where internet has revolutionized the world, it has also driven the life from being physical interaction to virtual world. The basic challenge in this scenario is to facilitate it with an instrument which can guide people to identify the differences between real and the virtual world. Smart cards have ensured that there is no need for physical presence. It's more of an authentication than the identification now. Individual credentials should be authenticated by a well-defined entity within the structured legal framework of all the user states. Securing all the individual credentials should be the top priority of all the administrators of smart card technology. Use of cryptographic technology is one of the recommended options to be exercised upon [35]. Since, security concerns demand that all the security measures should be progressive with evolving technology as it affects same both for malicious attackers and the users.

The main application approach with respect to smart card technology has now been driven from having a secured ID to multifaceted smart card applications which can offer not only the authentication for a an administrator, it should also assist the user to access a wide range of applications offered by the smart card technology. Focus gradually has shifted from the contact to contactless application in respect of smart card technology which facilitates the user to avail the various types of applications from a distant location. Radio frequency driven communication for the smart card applications is vital as it allows the transactions exercised by the cardholder and the administrator both. The objective of this technology is to bring upon a solution which can facilitate the provisioning of a single card to a user to use it not only as an authentication tool for him/her, it should also offer a viable option for many other applications [36]. Smart card exactly fits in this framework due to its inherent flexibility and security.

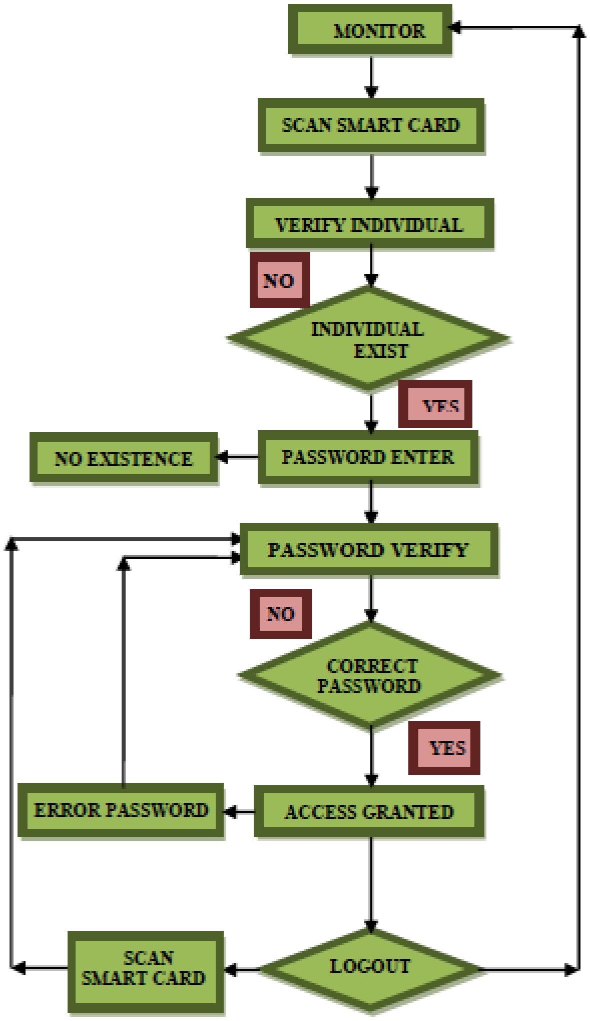

Fig. 4. Flow chart for smart card login.

In order to have the unambiguous understanding of functionality, let us have a look on a flow chart of a small application of a smart card as illustrated in Fig. 4 below. To access the database of any application for establishing the credentials, all individuals will be required to login. It can provide the required interface for all individuals in possession of smart cards to access the desired application. Initially, the user needs to scan his/her smart card through the designated card reader. The system then verifies the personal credentials of user from the database and if, the login ID exists, it asks the verification code which may be a PIN number or a password. In case the user's login credentials are verified, access is granted by the system. However, if login credentials of user do not match then the password/incorrect PIN whichever is applicable is reflected by the system with request to re-enter the access code [37]. This repetition of access is granted only for finite number of times or with restriction of certain seconds and thereafter the access of that smart card may invite temporary/permanent blockade of card.

This complete cycle of processing of authentication of a user of smart card has been shown below in the algorithm through a flow chart. This module can also be used for uploading of various subjected documents for a particular application provided that administrator of that application has granted that access right to that user. The distinct advantage of this access is that user does not need to carry all the documents all the time and they are available in the database repository of server which can be accessed at any point of time whenever needed by the user through his/her access rights.

The proposed algorithm is a basic system module which can be customized for any application of smart card technology based on the particular requirement of the organization/institution. To design a smart card application demands first to design the smart card with desired specification of the card itself [38]. A well thought out plan to be put on board regarding amount of data required to be stored, suitability of a particular application in the desired operation, kind of customization required in the existing tools, etc. The security concerns of the particular applications demands utmost attention. Adequate resources are required to be earmarked for exact authentication to the specific user so that rightful allocation of designated benefits can be assigned. Prevention of any unauthorized access is needed to be ensured. In all the arrangements where financial transactions are involved, a cap for every single as well as for the overall transactions must be exercised to rule out any kind of fraudulent or abuse against any individual or an institution. Our research approach is to propose a solution through smart card technology which facilitates in achieving the digital and cashless economy.

VII. Future Scope of Research Work

In last two decades a large amount of work has been put in development of smart card ID technology. Weather it is establishing an online authentication of a user, implementation of government run services or even execution of digital signatures, all these related issues have been dwelled in quite deliberation. Countries, like Germany, Italy, Mexico, Taiwan and many other countries worldwide are in the process of implementation of National E-Id. There is a need of elaborative plan to be adopted by all the countries whosoever are aspiring to implement it after thoroughly evaluating opportunities and challenges. A comprehensive guideline which is easy to assimilate by the user is required to be issued before implementation of such nationwide multipurpose smart card identity projects. The hardware involved must be cost effective with higher adoption rates in order to absorb the vast infrastructure during execution of such projects. There is a need to gain a good trust of the citizens for any country with easier use and larger acceptance before implementing such public projects.

To understand the software application dynamics of smart cards or its advantages over a computer based platform, we require a closer look of its evaluation in this respect. One most prominent advantage of smart card is its relatively quiet lesser vulnerability from Trojan horses or viruses/malwares compare to PC based platforms. Protection of data is ensured by stronger security mechanism in smart cards [39]. While any new smart card applications come in force, it is thoroughly evaluated and validated by independent certification agencies with respect to its provisioning or sustenance of degree of security. Since, the attackers too keep applying different methodology to find their way through the vulnerability of the system, there is a continuous requirement for an administrator using smart card technology to keep evolving themselves with latest threats or malpractices used by the attackers. Despite of a continuous evolving technology, there are certain points which can be identified as future scope for the smart card technology and these points are:

1) Focus on evolution of transistor technology of smart chip for better integration of new hardware applications. Due to space constraints, area required for inclusion of new circuitry in the chip is always a challenge.

2) Rate of power dissipation of smart card batteries too require adequate attention. A continuous endeavor to increase the battery life of smart card demands ample consideration in the design technology of its power circuits.

3) Credibility of any technology lies in its scope and reach to draw desired amount of benefit accrued out of this. It dictates to deliberate for a larger amount of applications of smart card technology for maximum gains to people. It must be ensured by a wide range of applications in all the walks of life.

4) Interoperability of smart card technology with other evolving technologies must be assured. Various networks operating in the complex internet environment have different communication protocols. Synchronization with these networks is the key for success of smart card technology [40].

5) The operating system of software used in this technology is another area which warrants desired amount of consideration. Smart card system requires an uninterrupted connectivity with other information systems in pursuit of matching pace with other evolving technology.

6) A concerted effort is needed to meet the challenges posed by an attacker on vulnerabilities of security threats on smart card technology both for hardware and software mechanisms.

7) Sensors, special material for design, alarm systems, inclusion of complex cryptographic algorithm, lower dimensional optimization are just the few other suggested areas which do require additional focus.

8) A consolidated single multipurpose global smart card ID to do away with all other kinds of identity requirements should be the ultimate aim of smart card technology [41]. It may necessitate associating various other evolving technologies with this to accomplish the desired outcome.

VIII. Conclusion

The emphasis on correct identification of every citizen is the basic proposition of all the sovereign governments across the globe. Perceived security threats to existing identification technologies are compelling factors to pursuit for evolving smart card technology. Security mechanism incorporating the complex encryption technology in place by this technology makes it more attractive compared to similar other available applications. This is a tool which offers to store and use the minimum desired data against a set of people or entity [42]. A suitable authentication scheme and security algorithm for faster and protected processing of data is always a challenge for any such technology. The above proposed study illustrates that user acceptance for constant evolving smart card technology will be the most prominent factor for the expected outcome. Further studies on the smart card system are likely to bring better dividends on issues as discussed in the subjects to be dealt with in above mentioned future scope.

Adaptability of this multifunctional technology in Internet of Things (IoT) with varieties of purposes makes it a lucrative proposition for commercial aspirants. Concerns on accessibility for both physical and logical control of the smart card applications are needed to be addressed adequately. The underlying intent of this research paper is to make the most of the smart card technology to exploit it to the fullest for the benefit of civilization. Endeavor is to combine all the existing traditional identity technologies and propose a workable single multipurpose identity supported by smart card technology [43]. Simplicity in use and robustness of the system must be assured in all the applications of this technology. A fundamental prerequisite for any modern technology including smart card technology increasingly relies on its adjustment with all accessible applications by of online services. The degree of convenience, cost effectiveness, multi-application solution and reasonable execution time for transactions are some of the few factors contributing in successful implementation of the smart card technology [44]. Above all, potential of this technology to replace all existing identity solution shall lead to a much desired instrument for all the government across the world to exercise their authority on their citizens and to ensure that all the warranted privileges to be driven to the deserving entities only. Implementation of a nationwide single multipurpose smart card ID will enable to carry forward the vision of having a worldwide single global ID for every user across the globe.

Acknowledgment

We are humbled to acknowledge the priceless guidance offered by Prof. (Dr.) Mukul Misra, Director (Research & Consultancy) Shri Ramswaroop Memorial University, Lucknow-Deva Road, 225003, U.P., India for this research paper. We are also indebted to Col A.K. Singh, Ph.D., Vice Chancellor, Shri Ramswaroop Memorial University, Lucknow-Deva Road, 225003, U.P., India for his precious guidance in making this paper in the desired shape. We record our deepest admiration of Col V.K. Tiwari, Ph.D. for his invaluable suggestions.

References

[1] Munizaga, Marcela A and Carolina Palma, “Estimation of a disaggregate multimodal public transport origin-destination matrix from passive smartcard data from Santiago to Chile" in Transportation Research Part C: Emerging Technologies 2012, vol. 24 pp. 11-17.

[2] Sven Vowe, Ulrich Waldmann, Andreas Poller and Sven Türpe, "Electronic Identity Cards for User Authentication Promise and Practice", IEEE Security & Privacy January/February 2012, vol.10, No. 1, pp. 48-53.

[3] Y. Wang and X. Ma, "Development of a data-driven platform for transit performance measures using smart card and GPS data" J. Transp. Eng 2014, vol. 140 no. 12 pp. 4026-4053.

[4] M. Batty, C. Zhong, J. Wang, E. Manley, F. Chen, Z. Wang and G. Schmitt, "Variability in regularity: Mining temporal mobility patterns in London Singapore and Beijing using smart-card data" PLoS ONE 2016, vol. 11 no. 2 pp. 1-15.

[5] M. Mesbah, A.A. Alsger and L. Ferreira, "Use of smart card fare data to estimate public transport origin–destination matrix" Transp. Res. Rec. J. Transp. Res. Board 2015, vol. 2535, pp.89-94.

[6] Y. Asakura, T. Kusakabe and T. Iryo, "Estimation method for railway passengers train choice behavior with smart card transaction data" Transportation 2010, vol. 37 no. 5, pp.732-747.

[7] C. Morency, M. P. Pelletier and M. Trépanier, "Smart card data use in public transit: A literature review" Transp. Res. C Emerging Technol 2011, vol. 19, no. 4, pp.558-567.

[8] Al Khouri A. M, ‘Targeting Results: Lessons Learned from UAE National ID Program“, Global Journal of Computer Application & Technology 2012, vol. 2, no. 1, pp.832-835.

[9] Albert Levi and Omer Mert Candan, “Robust Two-factor smart card authentication”, IEEE International Black Sea Conference on Communications and Networking (Black Sea Com) Year: 2017, pp.1-4.

[10] Jisung Kim, Hyongmin Lee, Taehoon Kim, Dongwoo Ha and Suhwan Kim, “Differentiating ASK Demodulator for Contactless Smart Cards Supporting VHBR”, IEEE Transactions on Circuits and Systems II: Express Briefs 2015, Vol 62, Issue: 7, pp.642-644.

[11] A. M. Ali and H. K. Lu, "Making Smart Cards Truly Portable," in IEEE Security & Privacy 2010, vol. 8, no. 8, pp.29-33.

[12] Latifa Oukhellou, Michel Verleysen, Mohamed K, El Mahrsi and

Etienne Come, “Clustering Smart Card Data for Urban Mobility Analysis”, IEEE Transactions on Intelligent Transportation Systems Year: 2017, Vol 18, Issue: 3, pp.714-725.

[13] Goswami A, Odelu V and Das AK, “A secure biometrics-based multi-server authentication protocol using smart cards”, IEEE Trans In Forensics Secure 2015, vol 10, pp.1962–1964.

[14] Moradi A, Schneider T, In Güneysu G and Handschuh H, “Leakage Assessment Methodology - A Clear Roadmap for Side-Channel Evaluations”, Cryptographic Hardware and Embedded Systems, Springer-Verlag, CHES 2015, volume 9293 of Lecture Notes in Computer Science; 496–511.

[15] Ashok Kumar Das, Kee-Young Yoo, Alavalapati Goutham Reddy and Eun-Jun Yoon, “Lightweight authentication with key-agreement protocol for mobile network environment using smart cards”, IET Information Security 2016, vol 10, Issue 5, pp.274-280.

[16] C. Kumar, W. Sharon Inbarani, Charlie Paul, G and Shenbaga Moorthi “An Approach for Storage Security in Cloud Computing- A Survey”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) January 2013, vol 2, Issue 1.

[17] Zhang QM, Ma CG and Wang D, “Cryptanalysis and improvement of dynamic ID-based authentication scheme”, in ICDCIT Springer: Berlin/Heidelberg 2012, vol. 7154, pp.143-151.

[18] Wu S and He D, “Security flaws in a smart card based authentication scheme for multi-server environment”, Wireless Personal Communications 2012; DOI: 10.1007/s11277-012-0696-1.

[19] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards", Information Security IET 2013, vol. 5, no. 3, pp.147-150.

[20] N.W. Lo, J. L. Tsai and T. C. Wu "Novel anonymous authentication scheme using smart cards", IEEE Trans. Ind. Informant Nov 2013, vol. 9, no. 4, pp.2006-2011.

[21] Wang C, X. Li, J W. Niu, J. Ma, W D. and L. Liu "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards", Journal of Network and Computer Applications 2011, vol. 34, no. 1, pp.74-78.

[22] K. B. Bey and F. Benhammadi, "EMBEDDED FINGERPRINT MATCHING ON SMART CARD", International Journal of Pattern Recognition and Artificial Intelligence 2013, vol. 27.

[23] Won D, Choi Y and Lee, Y, "Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction", Int. J. Distrib; Sens Netw 2016, pp.1-14.

[24] S.V.K. Llingeswaran and Arul Das, "GPS Based Automated Public Transport Fare Collection Systems Based On Distance Travelled By Passenger Using Smart Card", International Journal of Scientific Engineering and Research (IJSER) March 2014, vol. 2, issue 3.

[25] Ferreira L, Alsger AA, Safi H and Mesbah M, "Use of smart card fare data to estimate public transport origin-destination matrix Transportation research record", J Transp Res Board 2015, pp.89-94.

[26] Dobraunig C, Joye M, Mangard S, Eichlseder M and Moradand Mendel F, "On the Security of Fresh Re-keying to Counteract Side-Channel and Fault Attacks". In *Smart Card Research and Advanced Applications - 13th International Conference,* Springer - Verlag, *CARDIS 2014*, volume 8968 of *Lecture Notes in Computer Science*, pages 235–242.

[27] Chengzhong Xu, Fan Zhang, Lei Rao, Juanjuan Zhao, Chen Tian and Xue Liu, "Spatiotemporal Segmentation of Metro Trips Using Smart Card Data", IEEE Transactions on Vehicular Technology 2016; vol: 65, Issue: 3, pp.1139-1146.

[28] P. Venkatesh, R. Padmavathi, K. M Mohammed, Azeezulla, Mahato G, Kanchan Kumar and Nitin, "Digitalized Aadhar enabled ration distribution using smart card", 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) 2017, pp.616-617.

[29] K. Kyoungtae L. Inmook and M. Jaehong "Analyzing passenger's tagging behavior using smart-card data", Proc. of the 2014 Conf. of the Korean Society for Railway October 2014, pp.636-637.

[30] J. Y. Kuo and C. C. Chang, "An efficient multi-server password authenticated key agreement scheme using smart cards with access control" Proceedings of International Conference on Advanced Information Networking and Applications Mar 2005, vol. 2, no. 28-30, pp.258-259.

[31] P. R. White and M. Bagchi, "The potential of public transport smart card data", Transport Policy 2005, vol. 12, no. 5, pp.467-473.

[32] C. Seaborn J. Attanucci N. Wilson, "Analyzing multimodal public transport journeys in London with smart card fare payment data", Transp. Res. Rec. J. Transp. Res. Board Dec 2009, vol. 2121, no. 1, pp. 57-61.

[33] K. Markantonakis and K. Mayes, "Smart Cards, Tokens, Security and Applications", Springer, January 2008.

[34] S. Feng, J. Zhao C, Tian F and Zhang C. Xu, "Understanding temporal and spatial travel patterns of individual passengers by mining smart card data" Proc. IEEE 17th ITSC 2014, pp.2992-2996.

[35] Liu L, F. Zhang, C. Tian, J. Zhao, C. Xu and X. Rao, "Spatio-temporal segmentation of metro trips using smart card data", IEEE Trans Veh Technol Mar. 2015, vol. 65, no. 3, pp.1139-1147.

[36] M. Mesbah, A. Alsger, L. Ferreira and H. Safi,"Use of smart card fare data to estimate public transport origin–destination matrix", Transp. Res. Rec. J. Transp. Res. Board 2015, vol. 2535, pp.89-95.

[37] Premila Bai, T Daisy Rabara M, S Albert and Vimal Jerald, "An Adaptable Secure Smart Card Architecture for Internet of Things and Cloud Computing", IJRET 2016, vol. 5, pp.163-169.

[38] Etienne Come, Mohamed K, El Mahrsi, Michel Verleysen and Latifa Oukhellou, "Clustering Smart Card Data for Urban Mobility Analysis", IEEE Transactions on Intelligent Transportation Systems 2017, vol. 18, Issue: 3, pp.718-727.

[39] K. Michael Raj,T. Daisy, Premila Bai and S. Albert Rabara, "Elliptic Curve Cryptography Based Security Framework for Internet of Things (IoT) Enabled Smart Card", World Congress on Computing and Communication Technologies (WCCCT) 2017, pp.44-45.

[40] S. A. Suandi and V. T. De Zhi "Fingercode for identity verification using fingerprint and smart card",10th Asian Control Conference (ASCC) 2015, pp.1-5.

[41] R. Chakra, R. Lamrani, J. L. Lanet, G. Bouffard, A. Mestiri, M. Monsif and A. Fandi, "Memory forensics of a java card dump", in Smart Card Research and Advanced Applications, Paris; France, Springer 2014, pp.4-15.

[42] A. Bhaskar, L. M. Kieu and E. Chung, "Passenger segmentation using smart card data", IEEE Trans. Intell Transp Sys Jun 2015, vol.16, no.3, pp.1539-1546.

[43] Lai Tu,Juanjuan Zhao, Fan Zhang, Dayong Shen, Chengzhong Xu, Xiang-Yang Li, Chen Tian and Zhengxi Li, "Estimation of Passenger Route Choice Pattern Using Smart Card Data for Complex Metro Systems", IEEE Transactions on Intelligent Transportation Systems 2017, vol. 18, Issue 4, pp.792-800.

[44] Himanshu Thapliyal, Azhar Mohammad and S. Dinesh Kumar, "EE-SPFAL: A Novel Energy-Efficient Secure Positive Feedback Adiabatic Logic for DPA Resistant RFID and Smart Card", IEEE Transactions on Emerging Topics in Computing 2016, vol. PP, Issue: 99, p.1.