ISSN 2319 - 5975
Volume 13, No.1, December 2023 – January 2024
International Journal of Networks and Systems
Available Online at http://www.warse.org/IJNS/static/pdf/file/ijns031312024.pdf
https://doi.org/10.30534/ijns/2024/031312024

# Secure Transactions in a Chip: A Contemporary Review of Smart Card Innovations

**Sinchana Naik[1], Spandhana[2],Taniya K Bant[3],Omkar[4], Senthil Kumar R[5]**
Students, Department of Computer Science and Engineering[1,2,3,4]
Senior Assistant Professor, Department of Computer Science and Engineering[5]
[1]Alva's Institute of Engineering and technology,India,sinchananaik62@gmail.com
[2]Alva's Institute of Engineering and technology,India,spandhanan21@gmail.com
[3]Alva's Institute of Engineering and technology,India,taniyabant2@gmail.com
[4]Alva's Institute of Engineering and technology,India,omkarpanchakattimath1@gmail.comn
[5]Alva's Institute of Engineering and technology, India,senthil@aiet.org.in

Received Date : November 22, 2023 Accepted Date : December 14, 2023 Published Date : January 07, 2024

## ABSTRACT

Smart card technology has emerged as a powerful tool in the field of secure identification, authentication, and transaction processing. This abstract provides a comprehensive overview of smart card technology, highlighting its key features, applications, and benefits. Smart cards, also known as integrated circuit cards, are portable devices that incorporate a microprocessor and memory to securely store and process information. These cards have revolutionized various industries by enabling secure access control, secure payment transactions, and secure storage of sensitive data. The abstract begins by exploring the fundamental components and architecture of smart cards. It delves into the different types of smart cards, such as contact-based and contactless cards, and explains the communication protocols employed in their operation. Furthermore, the abstract discusses the extensive range of applications where smart cards have found widespread adoption. These applications include identification cards, payment cards, healthcare cards, transportation cards, and more. The abstract highlights the advantages of using smart cards in each of these domains, such as enhanced security, convenience, and interoperability.

**Key words:** Smart Card, Security, Adoption/Acceptance, Satisfaction, Privacy, Non-repudiation, Authentication, Integrity, Verification, Information Technology.

## 1. INTRODUCTION

Smart card technology is already being used in a variety of techniques throughout the world; nevertheless, the need of security in information technology has risen, particularly in applications involving data exchange and online transactions. Furthermore, research in security have been identified as a factor that may influence smart card adoption by information technology acceptance[1]. The major goal of this research is to analyze smart card security principles and estimate a result of security related smart card usage[2]. To that purpose, a survey of 640 university students was conducted to examine the security of smart card technology adoption[5]. Unlike the conventional magnetic stripe cards employed in Automated Teller Machines (ATMs), smart cards leverage a ground breaking approach to access control the integration of a Personal Identification Number (PIN)[21].

Smart cards are so-called because they include a microprocessor. Even these cards are occasionally meant to be "chip cards" or "integrated circuit cards." The chip card looks like a credit card that also functions as a computer.[4] Unknowingly, chip cards have become a critical component of human life. Chip cards are reliable instruments that give valid user identification, as well as multi-functional, low-cost devices that can be readily changed for both logical and physical access. Digital access management encompasses well-known principles such as password checking as well as more security is provided[20].

advanced cryptographic authentication procedures such as Windows login, remote Network access, network verification" physiological identification storage, and others. ID cards and building access management are examples of physical access control. chip cards are used in a variety of additional applications, including well-being and services, cards, banking (such as ATM Credentials),"network verification, prepaid phone cards, and identification (such as Citizen cards, Staff identification cards, and Subscription cards). telecommunications (mobile phone subscriber identification and administration), transit Passes e-Passports and physical access control, Bank notes, Motor vehicle licenses.

It is critical to emphasize that the underlying issues with chip card technology must be addressed before the technology can be further developed. Various research has produced ideas and models to characterize and evaluate user approval. Each of these models recognizes several factors that explains user acceptability. Security can impact user enjoyment and, as a result, user adoption of smart card technology, according to one study. The security principles for smart cards were investigated to estimate the relevance of security in smart card adoption. Smart cards are used to store the data on a secure chip, making them less vulnerable to skimming and fraudulent activities. They can even be linked to smartphones, wearable devices and IoT.

## 2. PROTECTION OF SMART CARDS

The bulk of smart card applications are security-related. Smart cards are significantly secure than regular printed cards or even magnetic stripe cards. Chip cards are used more commonly to authenticate transactions, regulate access to restricted locations, and confirm identify.

Because system users have admittance to the smart card, it has a high level of security. Because users control the security component, it is subject to assault by hackers, astute outsiders, bad insiders, or even committed and well-funded rivals. The storage technology used in smart cards has an influence on the security of the card as well as the whole system[19]. Some memory systems are distinguished by certain characteristics.

### 2.1 Protective elements of Chip Cards

The following elements are critical to chip card security:

- Visible security features
- Protective measures implemented in security chips to enhance security
- Built-in Security functionalities of Software Platform
- Built-in Security functionalities in communication infrastructure

### 2.2 Visually identifiable security characteristics of Chip cards

Security features easily comprehensible to individuals are present on smart cards. There are some elements that prevent smart card falsification. Although these measures do not secure the card's contents, they do stop misuse of the card for badge identification[10].

## 3. EXPLORING THE INTERCONNECTED ROLES OF SIM CARDS AND SMART CARDS

The Subscriber Identification Module (SIM) serves as a smart card integral to mobile phones, facilitating the unique identification of each mobile device within the network. Issued by the mobile network provider, each SIM card is endowed with a distinctive key. This unique key plays a pivotal role as the mobile phone encrypts data with it, enabling secure communication between the mobile device and its affiliated network. In essence, the SIM card acts as a cryptographic linchpin, ensuring the confidentiality and integrity of data exchanges in the dynamic realm of mobile communications[22].

## 4. SECURITY

Given the potential for manipulation and fraud, security emerges as a concern of critical when handling the smart cards, particularly when they hold monetary value. To protect from unauthorized access, the implementation of both user identification and access control becomes imperative in distributed computer systems. Smart cards offer varying security features to address this challenge, including authentication, encryption using single and triple DES algorithms, MAC checksums, and it uses secret codes like PINs. These measures contribute to enhancing overall security during the implementation of smart card systems[9].

### 4.1 Protective attributes of the chip card chip

The production process of smart card chips includes rigorous testing of the microcircuit. Once tested, the chip enters a secure mode where accessing the internal circuit becomes highly difficult. External parties are unable to directly access the memory or other internal components. Implementing any changes or executing operations on the chip requires a carefully planned project to prevent unauthorized access and potential attacks. For example, businesses are unable to derive the chip's functions by simply switching the conductor. Furthermore, the chip incorporates encrypted connections between its components, ensuring the integrity and confidentiality of data transmission. Smart cards are designed with circuits capable of detecting and recognizing external interference. These circuits can identify abnormal supply levels, extreme external frequencies, and excessively low operation temperatures, providing an additional layer of protection against potential threats.

### 4.2 Protective capabilities of the card operating system

To provide different levels of security and access control, smart card files can be protected using cryptographic keys or a Personal Identification Number (PIN). By implementing PIN-secured card access with fine-grained control over data entities, it becomes possible to develop diverse security policies for specific information segments[7]. This allows for customized protection and management of various data elements stored within the smart card. In order to safeguard against misuses the event of a lost or stolen smart card, PIN-enabled functionalities can be applies to the manipulation of data objects, including those achieved through programmable applications downloaded into the smart card. If an incorrect PIN is entered multiple times beyond a predetermined threshold, the activation of chip card is disabled. Some card issuers also possess the ability to reset a dormant smart card. The architecture of the smart card plays a critical role in ensuring data security and preventing unauthorized access or misuse[8].

### 4.3 Protective capabilities of the network's security measures

Data communication. should be adequately protected either through the system's design or the implementation of network protocols that prevent tampering and maintain the overall system security. Physical security measures can be implemented to secure the card terminal. For example, if the card terminal is integrated into a wall, the card security is ensured by utilizing equipment such as a smart card reader with a mechanized shutter[6]. Additionally, the communications connection and smart card reader can be physically safeguarded by placing them in a secure location. These measures contribute to protecting the integrity and confidentiality of system and its associated data.

### 4.4 Fundamental Security Concepts

Security is of utmost importance in a smart card system due to various factors. Upholding the principles of irrefutability, data consistency, identity verification, and verification are critical components of ensuring a secure environment[10]. These principles help to establish trust, prevent the denial of actions or transactions, maintain data accuracy and consistency, verify the identity of users, and validate the reliability of the system's operations[3]. By adhering to these methodologies, a smart card system can safeguard against unauthorized access, protect sensitive information, and maintain the overall security and reliability of the system.

These ideas are brought from various encryption algorithms used by smart cards. A single mechanism may occasionally be able to offer many security services. For instance, a digital signature can offer non-repudiation, source authentication, and data integrity[11]. Public key infrastructure (PKI) is important because it offers the policies and processes needed for creating secured information exchange, which is required for the majority of these security needs.

PKI (Public Key Infrastructure) utilizes data scrambling to ensure privacy, electronic certificate for verification purposes, and digital signatures to demonstrate the integrity of transactions performed by the originator without interruption or error. The upcoming sections will delve into the processes employed in smart cards to enforce these fundamental principles.

## 5. PRIVACY

The concept of safeguarding message exchanged between two parties from third-party interference is known as privacy. However, additional research on privacy and security is required before designing a card capable of preserving such confidentiality. This is because of heightened risk of privacy breaches when a person's smart card contains a larger amount of unique and personal information. Nonetheless, smart cards currently possess a diverse range of applications, and as they continue to shrink in size, become more affordable, and gain enhanced capabilities, their ability to support even more functions increases significantly.

Privacy is ensured using symmetrical and asymmetrical cryptography. Various procedures are required depends on card application. Numerous algorithms were implemented. is not conceivable despite the abundance of physical resources

It is common that a single algorithm will be universally employed. Currently, the widely adopted symmetric key cryptography algorithm is DES (FIPS 46-3), or potentially triple-DES (ANSI X9.17), while RSA is commonly utilized for asymmetric cryptography. Although it is unlikely to occur anytime soon, there might be future initiatives to replace DES with the more advanced AES (FIPS 196) algorithm

- Symmetrical Cryptography: Symmetrical cryptography employs A single key is used to encrypt plain text into enciphered text and to decode enciphered text back into plain text[12]. Cryptography with symmetry is called symmetrical because it uses the same. To encode and decode the communication the key is used. The DES algorithm is a fast method that may be utilized with smart card software. (FIPS 46-3) [13]. The conventional method for securely distributing keys to cards is to write a des key at the time of card personalization. Asymmetrical cryptography, which is described below If this is not achievable
- Asymmetrical Cryptography: In their article "New Directions in Cryptography," published in 1976, initially proposed separating the encryption/decryption key rather than using a single key for both functions. This concept is now recognized as asymmetrical cryptography. Two keys are used in asymmetric cryptography: one to encrypt plain text and the other to decrypt it. These are connected mathematically. The communication with only one key can be unlocked using a different key. RSA is popular asymmetrical cryptography algorithm[12].

This is used by credit card firms for authentication. Data encryption is rarely utilized. Asymmetric cryptography is also employed for this purpose. Asymmetrical encryptions are frequently used to safely transfer the key from one party to another. Asymmetric encryption is used for data transfer if both participants should know of the DES key. This action enhances the presentation.

### 5.1 Integrity

Data integrity is the confirmation via cryptographic methods that the communication conveyed from the sender to the addressee is accurate[14]. In actuality, Integrity of data guarantees that only individuals with proper authorization have access. may see or alter the data. A data integrity assurance ensures the message's content is accurate.

**5.1.1 Message Integrity Code**: Because an A message is assigned an 8-byte value. and a one-way cryptographic procedure is employed to construct the value, Mac is specific to that message.

The Mac character is added at last of a plain text message. before it is transmitted. When a message is delivered, the recipient computes the Mac value and compares it. If any modification is made to even a single character within the message, it renders the message invalid., the Mac modified in an unexpected way. The Mac gives the recipient peace of mind that the massage has not been interfered with[15]. It is essential that the messages sent between a smartcard and a smart chip reader be protected, by Mac.

#### 5.1.2 Non-Repudiation

The starting point of the data exchanged in the operation is confirmed via non-repudiation. The completed transaction cannot be disputed by any side. A particular communication delivered from a sender could never be rejected by a recipient. The communication is irrefutable to the receiver. Cryptography ensures that the transaction cannot be revoked

#### 5.1.3 Digital Signature:

To better grasp this functionality, let us prepare an illustration: Alice received a communication from Bob that is encrypted. Ram uses Sham's public key to encode the message, and Sham uses his private key to decode it[15]. Sham can use this characteristic to confirm that Ram truly sent the message. The foundation for electronic signature is this.

**5.1.4 Verification**:

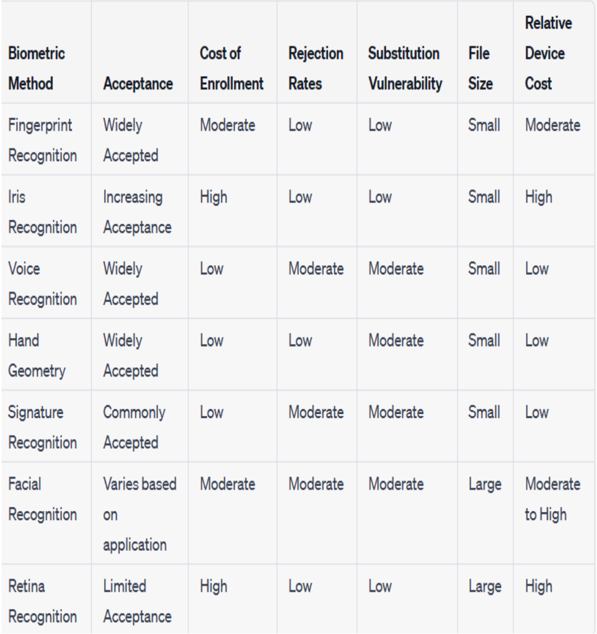
Verification is the method of determining a person's identification. In reality, it provides clarification or confirmation that a person or object is indeed the entity it claims to be. For instance, Ram needs to be certain that Sham is the processor of the key before accepting a communication from him. This requires a procedure known as authentication. Certificates: The authority that issues the certificate guarantees that the certificate's holder is who they claim to be. if the securely signed message contains a copy of the certificate holder's public key and other details about certificate holder. The recipient of the communication can then be certain that the key is trust-worthy[16].

The helpful action before using a card is verifying the cardholder's identification. If two parties wish to start a business, they must be certain of each other's identity. We can use verbal and visual cues to identify other people. To confirm that the person being impersonated is actually that person, secure communication technology.is used.

- Security codes: Security codes typically refers to a sequence of four or five digits. that is attached to the smart card. Cardholder commits this number to memory. PIN is securely kept. Digital content and functions on the chipcard can be secured until access from the outside world is permitted. Due to the excessive number of chip card applications, it will take some time until the proper pin code is available. As a result, people will need to memorize more and more pin numbers. Keep in mind that 15–20 distinct Security codes are challenging for everyone and could result in someone writing the secured number on the card. The initial merit of having a PIN was lost, which is why subsequent attention to security measures has focused on biometric as a method of recognizing a person.

- Biometrics: The science of quantifying characteristics is called biometrics. Users find it difficult to remember numeric pass codes and secret phrases. a determining component influencing the betterment of biometrics is this reluctance. Additionally, since many people share pin numbers, they are not identifiable uniquely, whereas biometrics can identify a real person since they are the following biological characteristics can be measured:
  - ➢Signature
  - ➢Fingerprint
  - ➢Voiceprint
  - ➢Hand geometry
  - ➢Eye retina
  - ➢visual identification

**Table 1**: Bio-Metrics methods in smart card technology



| Biometric Method | Acceptance | Cost of Enrollment | Rejection Rates | Substitution Vulnerability | File Size | Relative Device Cost |
|---|---|---|---|---|---|---|
| Fingerprint Recognition | Widely Accepted | Moderate | Low | Low | Small | Moderate |
| Iris Recognition | Increasing Acceptance | High | Low | Low | Small | High |
| Voice Recognition | Widely Accepted | Low | Moderate | Moderate | Small | Low |
| Hand Geometry | Widely Accepted | Low | Low | Moderate | Small | Low |
| Signature Recognition | Commonly Accepted | Low | Moderate | Moderate | Small | Low |
| Facial Recognition | Varies based on application | Moderate | Moderate | Moderate | Large | Moderate to High |
| Retina Recognition | Limited Acceptance | High | Low | Low | Large | High |

Table 1 shows the different biometric methods that can be used for smart card authentication, such as fingerprint recognition, iris recognition, and voice recognition.

## 6. PROPOSED MODEL

Three primary constructs-security, satisfaction, and adoption-are established in this research based on a survey of related literature. A research model is displayed, however, the study focuses on analyzing Data Capture models for the security construct[17].

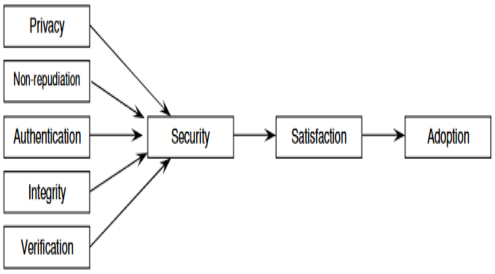


**Figure 1**: Flow diagram of Security in smart cards

Figure1 shows the relationship between various factors that influence the adoption of smart cards, including privacy, non-repudiation, authentication, security, satisfaction, and adoption.

### 6.1 Safety Dimension:

According to certain surveys, users' concerns about security have grown, and this has been identified as one of the main aim of technology aspect. In this study “degree to which person feels that security is important to them and believes that by using smart card is secured” is the definition of security. Strengthening system security will safeguard uses perception of the systems overall quality. security control may help to safeguard systems holistic content. Superiority by preserving the availability, confidentiality and integrity of the material[18].

## 7.METHODS

It appears that you are describing a study that used an online poll to collect data from university students who use smart cards. The researchers chose university students because they typically considered technologically good and well-informed. The data collection involved a total of 640 samples. The instrument used in the research consist of three sections. The first section gathered demographic information, while second and third sections included a set of twenty-five items measured sections of the questionnaire assessed satisfaction and adoption, as well as security measures. The satisfaction and adoption portion contained six measurement items, while the security section had thirteen measurement items. To analyze the data, the researchers used SPSS 16.0 for Windows software. They performed a factor analysis on all nineteen items, which included measures of security, satisfaction, and adoption. The researchers also calculated Cronbach's alpha, a measure of internal consistency, which indicates the reliability of the scale[19]. In this case, the Cronbach's alpha was found to be greater than 0.7, indicating that the scale satisfied the requirement for reliability.

## 8. CONCLUSION

Users must be able to trust a new system or piece of technology used in it. Being safe can therefore persuade customers to adopt new technologies, including smart card technology. outcome of the survey shows that most students (81.8%) believe smart card systems are secure since they have that perception. Furthermore, more than 90% of respondents said that security would be crucial when using a smart card. The outcome of this study demonstrate that security has a large and positive effect on user satisfaction and, consequently, on user acceptance. According to this statement, user acceptability will increase when security levels are increased[20]. Finally, further study will need to be conducted to find out factors that helps consumers understand the system and to develop fresh ideas for enhancing the security of smart cards.

## REFERENCES

[1] T. Li, D. Sun, J. Peng, and K. Yang, ‘‘***Smart card data mining of public transport destination: A literature review***,’’ Information, vol. 9, no. 1, p. 18, Jan.

[2] I. Al-Alawi, & M.A. Al-Amer, “***Young Generation Attitudes and Awareness Towards the Implementation of Smart Cards in Bahrain: An Exploratory Study***”. Journal of Computer Science, Vol. 2 No. 5, 2006, pp. 441-446.

[3] Carol Hovenga Fancher, “***In Your Pocket: Smart Cards***”,IEEE Spectrum, February 1997.

[4] M Bagchi and P. White, ***‘‘What role for smart-card data from bus systems?’’*** Municipal Eng., vol. 157, no. 1, pp. 39–46, 2004.

[5] P. T. Blythe, ***‘‘Improving public transport ticketing through smart cards,’’*** Municipal Eng., vol. 157, no. 1, pp. 47–54, 2004..

[6] M.-P. Pelletier, M. Trépanier, and C. Morency, ***‘‘Smart card data use in public transit: A literature review,***’’ Transp. Res. C, Emerg. Technol., vol. 19, no. 4, pp. 557–568, 2011.

[7] X. Ma, C. Liu, H. Wen, Y. Wang, and Y. Wu, ***‘‘Understanding commuting patterns using transit smart card data,’’*** J. Transp. Geogr., vol. 58, pp. 135–145, Jan. 2017.

[8] Phil Blythe, ***“Integrating Ticketing-Smart Card In Transport”,***IEEE Colloquium:UUsing ITS in Public Transport and in Emergency Services, December 1998.

[9] C. Zhong, E. Manley, S. M. Arisona, M. Batty, and G. Schmitt, ***‘‘Measuring variability of mobility patterns from multiday smart-card data,’’*** J. Comput. Sci., vol. 9, pp. 125–130, Jul. 2015.

[10] Karin Schier, ***“Multifunctional Smart Cards for Electronic Commerce- Application of the Role and Task Based Security Model”***, Computer Security Application Conference, December 1998.

[11] Q. L. Gao, Q. Q. Li, Y. Yue, Y. Zhuang, Z. P. Chen, and H. Kong, ***‘‘Exploring changes in the spatial distribution of the low-to-moderate income group using transit smart card data,’’*** Comput., Environ. Urban Syst., vol. 72, pp. 68–77, Nov. 2018.

[12] J. B. Ingvardson, O. A. Nielsen, S. Raveau, and B. F. Nielsen, ‘‘***Passenger arrival and waiting time distributions dependent on train service frequency and station characteristics: A smart card data analysis,***’’ Transp. Res. C, Emerg. Technol., vol. 90, pp. 292–306, May 2018.

[13] W. Tu, R. Cao, Y. Yue, B. Zhou, Q. Li, and Q. Li, ***‘‘Spatial variations in urban public ridership derived from GPS trajectories and smart card data***,’’ J. Transp. Geogr., vol. 69, pp. 45–57, May 2018.

[14] H.-M. Sun, ‘‘***An efficient remote use authentication scheme using smart cards***,’’ IEEE Trans. Consum. Electron., vol. 46, no. 4, pp. 958–961, Nov. 2000.

[15] Yang, D. S. Wong, H. Wang, and X. Deng, ‘‘***Two-factor mutual authentication based on smart cards and passwords***,’’ J. Comput. Syst. Sci., vol. 74, no. 7, pp. 1160–1172, Nov. 2008

[16] T. Limbasiya, M. Soni, and S. K. Mishra, ‘‘***Advanced formal authentication protocol using smart cards for network applicants,***’’ Comput. Electr. Eng., vol. 66, pp. 50–63, Feb. 2018.

[17]. D. Zhao, W. Wang, C. Li, Y. Ji, X. Hu, and W. Wang, ‘‘***Recognizing metro bus transfers from smart card data***,’’ Transp. Planning Technol., vol. 42, no. 1, pp. 70–83, Jan. 2019

[18]. J. Zhao, F. Zhang, L. Tu, C. Xu, D. Shen, C. Tian, X.-Y. Li, and Z. Li, ‘‘***Estimation of passenger route choice pattern using smart card data for complex metro systems***,’’ IEEE Trans. Intell. Transp. Syst., vol. 18, no. 4, pp. 790–801, Apr. 2017.

[19] J. Li, Y. Lv, J. Ma, and Q. Ouyang, ‘‘***Methodology for extracting potential customized bus routes based on bus smart card data,***’’ Energies, vol. 11, no. 9, p. 2224, Aug. 2018.

[20] Hamed Taherdoost, Shamsul Sahibuddin, Neda Jalaliyoon, “***Smart Card Security; Technology and Adoption***” International Journal of Security(IJS), Volume(5):Issue (2):2011

[21] X. Li, J. Niu, M. Khan, and J. Liao, ‘‘***An enhanced smart card based remote user password authentication scheme***,’’ J. Netw. Comput. Appl., vol. 36, no. 5, pp. 1365–1371, 2013

[22] Q. Jiang, J. Ma, G. Li, and X. Li, ‘‘***Improvement of robust smart-card based password authentication scheme***,’’ Int. J. Commun. Syst., vol. 28, no. 2, pp. 383–393, 2015