Volume 13, No.1, December 2023 – January 2024
ISSN 2319 - 5975
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.comm
[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