CGC International Journal of Contemporary Technology and Research
ISSN: 2582-0486 (online) Vol.-3, Issue-2 DOI: 10.46860/cgcijctr.2021.06.31.158

Wi-Fi Security Card (WCS): A Novel Approach for Secure Payment System

Sumit Kumar
Department of Computer Science and Engineering
Chandigarh Group of Colleges, Landran
Email Id: *cse.kumarsumit@gmail.com

Abstract:-**The latest technology is turning into a vital element in financial business. This paper presents a proposed system called Wi-Fi Security Card (WCS) based on the very common and growing problem of electronic transaction fraud in the countries of India. To solve such problems, we have proposed a novel secure payment method known as Wi-Fi Security Card (WCS). In this paper, we also compared the WCS system to another existing system called Dropped Card Detection (DCD) and Microcontroller and Sensors (MAS). The main advancement of our system over the existing system is that WCS can also prevent fraudulent transactions. Nowadays, security issues in e-payments are usually more demanding than current security issues on the internet. Our findings may enable e-transaction providers to extend their secure payment systems by increasing their protection as necessary for appropriate financial services.**

Indexed Terms**- WCS, Smartphone, Secure Payment, App**

I. INTRODUCTION

The e-payment method has continued to develop more and more in the past years due to the increasing demand for web-based banking and shopping [1]. The idea behind this paper is "Prevention is better than Cure". We are always taught to take care of ourselves and our things or we will regret later. Our app works best for these words. It will provide instant security to Wi-Fi enabled credit/debit cards during the transaction. It is a simple software application that will be installed on the Smartphone of user. User will enter their account number, account holder name, and the registered mobile number. The secure and user-friendly payment process improves the use of electronic transactions [2]. After this user can add the mobile numbers of the people who may use their card. Now, this depends on the user whether they want to give authentication to that person by selecting the number from the list present in the WCS application or not. For example, if a family member of the user wants to use his Wi-Fi enabled credit or debit card then the user will select her number from the list of added mobile numbers.

Whenever a transaction will be requested from the card a "security alert" message will pop up on the screen of the person whose mobile number is currently selected at that time in the application by the user. E-commerce is the development of electronic means of transaction [3]. This popup will appear for a short period in which the user has to choose the 'YES' or 'NO' option otherwise after time out, the transaction will be declined.

If the transaction is requested by the person using the card, they can click 'YES'. If the user is unaware of that transaction or has lost his card, or the user senses some illegal use of the card then the transaction will be denied by simply clicking 'NO'. If the user was busy with some task and is not aware of unauthorized transactions and not able to see the prompt message then those transactions are automatically denied after a short period. This ensures that no fraudulent transactions take place and users will feel secure about money all the time. Customers often reveal data that is private which is for example their name, card number, and any other data during their online transactions [4]. WCS ensures security at every step. Even if the Wi-Fi-enabled card is lost, dropped, or stolen, no transaction can be authenticated without the users' consent.

Fig. 1. Application interface of WCS

NOVEL FEATURES:

- Easy to use.
- Instant payment after authorization.
- May be used by multiple people selected by the user.
- Provides record of transaction.
- Cost-efficient.
- Time-efficient.
- Instant security.
- Prevents unauthorized transaction.
- Prompt message saves time and proceeds with secure transaction.
- Users can control the transaction even if the card is stolen or lost.
- Provides 24*7 securities.
- Control over transaction by simply clicking YES/NO.

ADVANTAGES:

- Helps people make a safe transaction.

- Cost-effective.
- Reduces the stress of losing the card.
- Provides security on the spot.
- No transaction can be made without the users' consent.
- Easy to use

This paper is divided into five different sections. Section 1 introduces the WCS system with its novel features and advantages. The rest of this paper is structured as follows. Section 2 describes related works with respective approaches. In section 3, the objectives of the proposed system have listed. Section 4 compared the projected system with the existing system and discussed the proposed methodology. Section 5 concludes the paper with the future scope.

II. RELATED WORK

P. P. Vishwakarma et al [5],An empiric path towards fraud detection and protection for NFC-enabled mobile payment system (2019): This paper presents the concept of an NFC-enabled electronic transactions fraud detection scheme. This scheme will analyze payments, assess every transaction for fraud or risk, and make appropriate choices.

D. Kumaret al [6], Electronic Payment System, Risk And Security Issues (2019): This paper focuses on protecting electronic transactions from a consumer point of view. As the consumer access to the security of electronic transaction methods has become a core aspect of the extension of the e-commerce market.

E. Modesta et al [7], Secured Online Transaction (SONT):Analysisand Solution Of Secure Electronic Transaction (2020): In this paper, the authors propose a Secure Online Transaction (SONT) system. The SONT system is used to introduce variable keys that validate the cardholder and merchant details prior to permission using a 2-way verification process.

KyawZayOo et al [8], Design and Implementation of Electronic Payment Gateway for Secure Online Payment System (2019): The authors have created an electronic payment gateway system for Secure online transactions. In this method, the financial information of the consumer (debit or credit card) is sent straight to a payment gateway called a trusted third party (TTP), rather than being sent through an online merchant.

Z. Bezhovski et al [9], The Future of the Mobile Payment as Electronic Payment System (2016): This paper proposes an electronic mobile payment system that will assess the current status and development of electronic transactions in markets worldwide and keep an eye on the future of this industry. The authors review several methods of mobile payment services and security issues associated with them and the future of electronic transactions.

Dynamic transaction card protected by dropped card detection (DCD):

The dynamic transaction card contains several interconnected layers. When the card falls off, the sensor layer in the card initiates the microcontroller activity that notifies the user about the fall of the card. The notification is sent on the Smartphone and the cardholder is requested to deactivate it.

A dynamic transaction card includes many sensors. It includes LEDs or light pipes embedded in the card, a sensor that detects dropped card, microcontroller, a printed circuit board (PCB), Near Field Communication (NFC) antenna or Radio Frequency Identification antenna (RFID), accelerometer, pressure sensor, and piezoelectric sensor. These are the sensors present in the card layers and help to detect the dropping of the card

III. OBJECTIVES

i. The main objective of this project is to provide instant security while a transaction is made.
ii. This app saves time and prevents the chaos created if the card is lost or an unknown transaction is made.
iii. Another objective of using this app is to make people more control over their transactions using WCS "Security alert" Yes/No.

IV. PROPOSED METHODOLOGY

When used for electronic transaction methods, the cloud application is used to accept and process transactions over the Internet rather than using a physical card [10][11]. In this paper, we have proposed a secure payment system app. The app will be installed on the Smartphone of user. The user will enter the Account number, Account holder Name, and the registered mobile Number.

Now whenever a user will use the card a "Security alert" prompt message will appear on the phones' screen having YES and NO as options. If the user selects YES the transaction will be authenticated otherwise declined. Moreover, user can add the mobile number of the people who may use his card.

TABLE I. COMPARISION OF PROPOSED WCS WITH DCD AND MAS

Name of the prior art	Key features of prior art	Key features of our invention
DCD	It is used to detect the card free fall. The card itself contains several protective layers including an outer protective layer; a secure payment chip, a microcontroller, a sensor, a near field communication (NFC) antenna, and an energy storage component to power a dynamic transaction card. After detection of a dropped card, it sends the notification to the user to deactivate the card.	WCS application provides instant security. It gives the user the control to prevent the transaction if the card is lost or stolen. Users can add the numbers of the people in the WCS application who may use the card other than him/her.
MAS	Sensors are applied to detection work.	Prompt message requests with user authentication.

User authorized people will also get the "Security alert" prompt message for proceeding with the payment by selecting the mobile number on the app by the user. Now assume that the card has been lost or stolen but the

transaction will not happen because the transaction requires authentication via the WCS app, which can only be done by the user.This system has several advantages for people accepting payments in terms of both data security and consumer experience [11][12]. As technology is progressing, it is making life fast and saves a lot of time.

TABLE II. LIMITATIONS OF DCD AND MAS

Name of the prior art	Key features of prior art	Key features of our invention
DCD	It only contains the feature to detect card free fall. Stealing of card cannot be detected. A person who stole the card can make the transaction and there is no feature to prevent this.	WCS is simple software that prevents fraudulent transactions at the transaction time itself. If the user confirms the payment, the transaction is authenticated but if denied, the transaction gets canceled. Even if the card is dropped or stolen, the user can control its use.
MAS	This technology uses numerous sensors which are very costly and require maintenance.	We can overcome this by using our WCS app. It cuts off the high cost of sensors and thus cost-effective.

With this, the security issues are also increasing. People want to be quick but also want a reliable technology. If a person loses his Wi-Fi-enabled credit/debit card, there is the full possibility that at least one transaction will be made without his/her consent. Users can block his card by contacting the bank but by the time he would have lost some money. Our app will provide instant security. Even if the card is lost or stolen no transaction can be made against the users' wish. The prompt message that will appear on the phone screen with YES/NO as the options will provide security and also save time. So it will be a reliable technology that saves time and provides instant security.

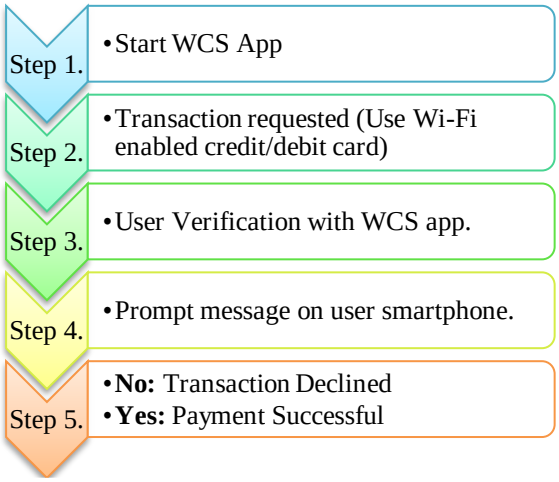

Fig. 2: Steps to verify transactions using WCS

WITHOUT WCS METHOD:

When a person use their Wi-Fi enabled credit/debit card for the payment of less than Indian Rupees 2000, no any PIN is required and the money is deducted automatically. It tends to save time. But in reality, if their card is lost or stolen, it is quite obvious that the person who got the card can make transactions before a person get to know about it and make attempts to block their card.

- Transaction Requested:When Wi-Fi enabled credit/debit card the transaction is requested but no authentication is checked.
- Payment successful:The money gets deducted from ones account. Even the person who stole his card is using it the payment will be authenticated.

By the time a person will realize that card is not with him and that person will contact the bank to block his card, the probability is that at least one transaction would have been authenticated without his consent. Presently, this is the scenario of a Wi-Fi enabled credit/debit card without security features.

WITH WCS METHOD:

Using a Wi-Fi card security application (WCS) a person gets security at every step of his transaction.

- Transaction Requested:When a person use his Wi-Fi enabled credit/debit card the transaction is requested and the authentication is checked using the WCS.
- Prompt Message:When the transaction is requested then the prompt message appears on the screen of his Smartphone asking Yes/No for proceeding with payment.
- YES/NO choice:If a person is using the card then by clicking yes that person can make a successful payment.

If that person does not want to proceed simply click no and his payment will be declined.

Now if his card is lost or stolen that person can still control his transactions and need not rush to contact the bank. When the person who got his Wi-Fi enabled card will request a transaction from the card that person will get the prompt message and can decline the transaction by choosing 'No'.Also if that person is unaware about stealing his card, still the other person cannot make a payment because if none of the options (Yes/No) will be chosen, the transaction will automatically be declined. This is so because the prompt message will appear for a short period, if that person is busy and did not acknowledge the prompt message it will decline the transaction after time out.

The Internet is a slightly less secure and unreliable way to perform any such transaction [11]. Since one can control transactions at any time using WCS, they can remain calm even if the card is lost or stolen. Even if that person provides his card to someone to use it, they will also get the prompt message for authentication if that person adds their number in the WCS app. For this, one can follow a simple procedure in the application that they have to add a number of that person.The purpose of user authentication is to confirm or disprove the identity of a person[13][14].

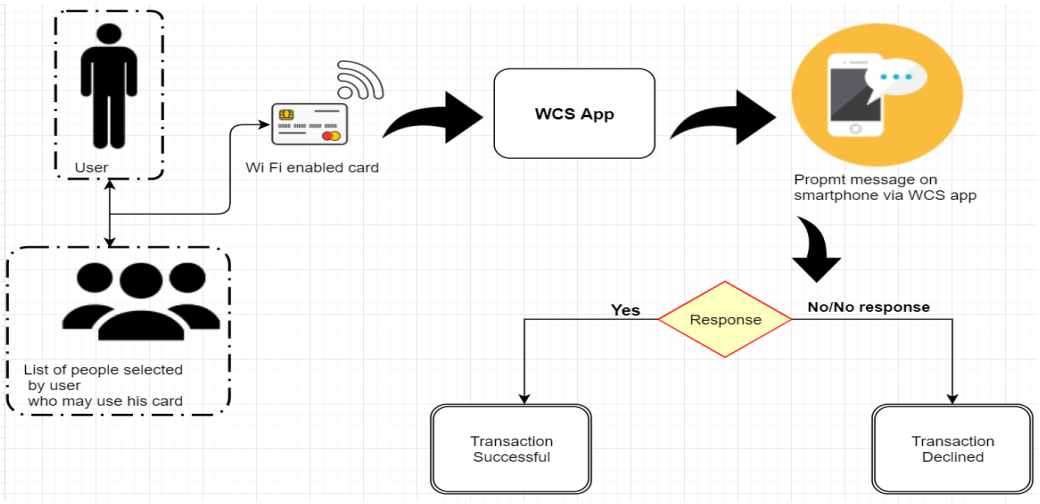

Fig. 3. Working diagram of the proposed system WCS

A list will be generated in the WCS app having the mobile numbers of the people who may use his card. Whenever any of them uses the Wi-Fi enabled card to make a transaction then the user will select that number from the list in the app and the prompt message will be sent to that number. Also it is not a matter of worry if the user forgets to select a number from the list because then by default prompt message will go to the registered users' number.

V. CONCLUSION

This paper presented the features that can achieve to create a secure payment system known as Wi-Fi Security Card (WCS) system. There are some problems in the current Dropped Card Detection (DCD) and Microcontroller and Sensors (MAS) system that can overcome with the proposed WCS system as discussed. The idea of launching this app is to make countries like India free from electronic transaction fraud. In the future, the card transaction verification method will be created in mobile real-time by reducing the waiting time for instant messages on mobile.

REFERENCES

[1] M. A. Hassan, Z. Shukur, M. K. Hasan, and A. S. Al-Khaleefa, "A review on electronic payments security," Symmetry (Basel)., vol. 12, no. 8, pp. 1–24, 2020.

[2] B. Jain and L. Bhatia, "Electronic Payment System : Effects of Transaction Procedures on Consumers ' Perceived Security," vol. 10, no. 02, pp. 6–8, 2019.

[3] M. Vadivel, "Sensitive Online Transaction Process," vol. 187, no. May, pp. 133–134, 2016.

[4] M. Naeem, M. Hameed, and M. S. Taha, "A study of electronic payment system," IOP Conf. Ser. Mater. Sci. Eng., vol. 767, no. 1, 2020.

[5] P. P. Vishwakarma, A. K. Tripathy, and S. Vemuru, "An empiric path towards fraud detection and protection for NFC-enabled mobile payment system," Telkomnika (Telecommunication Comput. Electron. Control., vol. 17, no. 5, pp. 2313–2320, 2019.

[6] D. Kumar, "Electronic Payment System , Risk and security issues," vol. 6, no. March, pp. 1–7, 2019.

[7] I. U. M, O. O. C, E. Modesta, I. Chidinma, and U. B. Chimezie, "Secured Online Transaction (SONT): Analysisand Solution Of Secure Electronic Transaction .," vol. 15, no. 2, pp. 32–39, 2020.

[8] Kyaw Zay Oo, "Design and Implementation of Electronic Payment Gateway for Secure Online Payment System," Int. J. Trend Sci. Res. Dev. Int. J. Trend Sci. Res. Dev., vol. 3, no. 5, pp. 1329–1334, 2019.

[9] Z. Bezhovski, "The Future of the Mobile Payment as Electronic Payment System," Eur. J. Bus. Manag., vol. 8, no. 8, pp. 127–132, 2016.

[10] S. K. Gurpreet Singh, Sunil Chawla, Shivangi, "Moving from databases to Cloud Database: Futuristic Trends 1," CGC Int. J. Contemp. Technol. Res., vol. 1, no. 2, pp. 12–16, 2019.

[11] V. Sindhu, "A Novel Approach to Automated Centralized e-Challan System for Traffic Management," CGC Int. J. Contemp. Technol. Res., vol. 2, no. 2, pp. 131–133, 2020.

[12] F. Mehmood, I. Ullah, S. Ahmad, and D. H. Kim, "A novel approach towards the design and implementation of virtual network based on controller in future iot applications," Electron., vol. 9, no. 4, 2020.

[13] F. Wang et al., "Identity authentication security management in mobile payment systems," J. Glob. Inf. Manag., vol. 28, no. 1, pp. 189–203, 2020.

[14] A. Pešterac and N. Tomić, "Loss of privacy in electronic payment systems," Anal. Ekon. Fak. u Subotici, vol. 56, no. 43, pp. 135–149, 2020.

.