The study of Cashless money transaction through wrist band

Mahalakshmi M, Pallavi Y,Priya Bharti,Manoj M
[1,2,3,4]Student,
[1,2,3,4]Information Science and Engineering,
[1,2,3,4]R V Institue of Technology and Management, Bengaluru,India

Abstract - Revolution in the economy has been achieved with the major contribution of cashless technology. This technology helped in transforming from hard cash payments to electronic payments. Digital transfer of money helps in the physical cash management. In this paper, we explained the concept of transferring the money digitally using Bluetooth module, additional authentication is provided using the fingerprint sensor and face lock. The payments through Unified Payment Interface (UPI) have several problems like application maintenance issues, server not found, phishing, request money fraud, misleading UPI handles. Also, the UPI transaction requires an active connection to the internet. The wristband transaction of money solves the problem by using proximity technology.

Index Terms - Fingerprint sensor, Digital money, UPI, Cashless technology

I. INTRODUCTION

With the increasing popularity of wearable technology, the possibility of cashless transactions through a watch has become a reality. This technology has the potential to revolutionize the way we make payments, providing us with a convenient, secure and fast mode of payment. A cashless transaction is the exchange of goods and services without the use of physical cash.

In this regard the idea of designing the wrist band for the cashless transaction has been presented. One of the most significant advantages of using a wrist band for payment transactions is the convenience it provides. Users can make payments without taking out their mobile phones, which can be especially helpful in situations where carrying a phone may not be practical or safe, such as when running or cycling.

This research paper will examine the potential benefits of using wrist band for cashless money transfers. These benefits include convenience, security, and accessibility. Additionally, this paper will explore the challenges associated with this technology, including compatibility issues, security concerns, and user adoption.

Here we make use of microcontrollers, Bluetooth modules, Fingerprint sensors. Bluetooth module helps in the direct transaction to receiver without intervention of third-party services. Microcontroller used for the easy to interface with the external devices like sensors and other devices connected to it. In the view of security, we make use of biometric authentication like fingerprint sensors to identify the right user during payments. An OLED to display the messages.This system is one of the efficient ways for the client-to-client transaction, small business payments, marketplaces money transfers where the payments are done in the smaller range.

In conclusion, the rise of technology has transformed the way we conduct transactions and make payments. The introduction of cashless payment systems has made our lives easier, more convenient, and more secure. The use of wearable technology such as watches to facilitate cashless money transfers is a promising development in the financial technology industry. As this technology continues to evolve, we can expect even more innovative solutions that will make our lives easier and more convenient. In this paper, we will explore the various aspects of cashless money transfer through watches and its implications for the future of payment systems.

II. LITERATURE SURVEY

Administration of client enhancement should be done through digitalization .By the means of digitalization the time will be getting saved and human mistakes will be diminished. Another advantage is how the bank responds to these innovations mainly in a positive way. For the digitalization client and banks need to work together. And it's their duty to be serious when they are working together.

The new presentation of open banking and the Payments Services Directive 2 (PSD2) guideline is rushing this change by putting power in the possession of clients .The new guidelines help the client in so many ways. Previously They were not allowed to share their monetary information. Now the bank is giving the permission to share their monetary information, how to manage the money and how to do the payments. Previously the banks were not ready for the colossal change because of the risk they might have suffered in the future. With the expanding use of cellphones, banks become the biggest shoppers of the monetary items. As a human there will be so many blunders that should have been done before , the digitalization helps in reducing those blunders Now the bank has only one risk that is to manage computerized attacks. [2]

Anywhere in the part of the countries, but mainly in India , the use of the fake currencies has been increasing rapidly and many of the fake currencies will not be getting detected. It is known that there are limits in printing the currencies by the government officials. Printing fake currencies is a crime against the government rules. By looking at all those past crimes now it's country duty to move away from the cash to the cashless payment .Cashless payment is a way where the goods are brought in exchange of payment through the electronic devices like cell phones . Cashless payment has so many advantages like the physical circulation is not needed. Now the developed countries have been increasingly moving from cash to cashless payment through electronic devices. [5]

The Development and how the cards have evolved is discussed in the literature survey because of the defaults in the previous cards. The very first transaction happened in 1987. There were two kinds of card transactions that had taken place at that time. First one is contact-based smart cards and second is contactless wristband cards. In those days the security was not enhanced . Contact-based consists of two parts, the first part is a magnetic strip and the second part consists of three tracks of data. Both of the magnetic strips consist of information about the name of the account holder , card number, card expiry date, country code etc. All these things were in encoded form because of the security purposes. The second type of contactless card is more secure than the previous one . This one is having the chip inside it. The chip is called a small processor .The wristband chips consist of Crypto Processor , Random Access memory, Read Only memory etc. These things are used for the generation of the security keys . The use of contactless payment over contact-based payment because of the special type of crypto process present in it. In the past lots of security attacks happened . The evaluation takes place fast from the magnetic strip to the NFC cards. The use of the NFC cards comes with so many risks . If the card has been stolen then without the requirement of the PIN and the OTP the transaction will get completed. So it’s becoming a challenging factor, to overcome this issue there should be some authentication factor that must be enabled for the transaction. So the wristband concept is one of them that comes into the picture. In the market the wristband is able to do the transaction but there is no authentication included in that. This wristband comes with a biometric sensor which is helpful for the authenticated transaction. So the ideas differ from the previous ones.

The main contribution of this project is to create a Point of Contact (POC) to show how the payment is done through the NFC and the fingerprint. Smartwatch that has pre-enables NFC and fingerprint sensor in it. The aim of this project is to make a transaction using the enabled Near Field Communication and the Fingerprint sensor hardware included in it. Nowadays wrist bands and other kinds of electronic devices lack security. The drawbacks will be overcome by including the biometrics sensor inside it. The wrist band with the fingerprint sensor supports high security in the digital environment . One of the serious issues is most of the NFC enabled cards and the other wearable devices will not be asking for PIN and OTP during the transaction. This issue will be getting resolved by adding the biometric sensor, like fingerprint before the transaction starts for the authentication and the verification of the user . This type of system has more advantages than the previous one. The main advantage is that the transaction will not get started without the user authentication. Once the user will give the authentication then only the payment process will be initiated and the transaction will be getting completed. This thing is new to the system that every time when the user will give the authentication then only the transaction happens. the fingerprints. There are so many advantages to wrist band watches, it is easy to carry and we don’t have to worry about it getting stolen . Since this is so small and wearable so no need to worry about getting stolen. It is also secured by the user fingerprint and crypto processor inside it for the authentication and the security purposes.[1]

Biometric authentication systems first require an enrollment phase, in the enrollment phase the user biometric measurement is taken place at first and saved in the device as a template. When the user attempts to authenticate the new measurement has been taken and it will be matched against the template. If both matched the user can initiate the payment process .

The use of biometric sensors provides one-to-one identity mapping for the security purposes. So the biometrics cannot be shared between the users. But such attacks are possible like mimicry attacks are typically feasible when it will have a sufficient amount of resources.

Now let us consider a system model in which a user is wearing a wrist band on his wrist and it starts to make payment through NFC enabled in it, in the shop or at the transport systems. For making the payment the user has to make the tap gesture. This is done when the user will be moving his hand towards the terminal until the watch is near to exchange the data by the means of NFC. The contact point of the NFC is when the payment provider would decide whether to approve the payment or cancel the payment process. [4]

There are so many new ways that happen for mobile payment systems. Wireless and proximity technology implementations are some of them. The capacity and power for the short-range device such as Bluetooth . Bluetooth is wireless and the communication medium between the two devices. Bluetooth is widely available for the transmitting and receiving data over the short distance between two electronic devices. [3]

The current generation is dependent on wrist bands. Because they need the installation of the apps and for the administration purposes . They only operate independently once the setup is done. There are two separate models that have been created by us: an authentication model, in which the authentication of the user will be done, and an intent recognition model, in which the payment will be initiated and the transaction will be completed. For the latter, we assume that a tap, such that if we identify a tap gesture during a transaction then we infer that the payment is intentional and the process of transaction will be initiated. The combination of these models forms our system, which we call WatchAUTH. [4]

III. EXISTING SYSTEM

There are many various systems for cashless money transfer available today in the modern world. Some of the examples include:

• Bank transfer: A bank transfer is a mode to send money from one bank account to another. It can be done through a bank's online platform, mobile app, or in person at a bank branch. To make a bank transfer, you will need to provide the recipient's name, bank account number, and routing number. The transfer can be initiated by the sender or the recipient, and the funds are typically available in the recipient's account within one to two business days.

• Mobile payment systems: Mobile payment systems facilitate users to make payments using their wrist band. To use a mobile payment system, you will need to set up an account and link it to your bank account or debit card. Then, you can use your smartphone to make purchases at participating retailers, send money to other users, or make other types of payments. Mobile payment systems use near-field communication (NFC) technology to transmit payment information wirelessly. Few examples of mobile payment systems include Apple Pay, Google Pay, and Samsung Pay.

• Digital payment apps: Digital payment apps are standalone applications that allow users to send and receive money, usually through a linked bank account or debit card. These apps often have additional features such as the ability to request money from others or split payments.Few examples of digital payment apps include PayPal, Venmo, and Square Cash.

• Cryptocurrencies: Cryptocurrencies are digital currencies that use cryptography for secure financial transactions. They operate on a decentralized network, meaning that they are not controlled by a central authority such as a bank. Cryptocurrencies can be used to make purchases or exchange them for other currencies. Few examples of cryptocurrencies include Bitcoin, Ethereum, and Litecoin. 6

• Prepaid debit cards: Prepaid debit cards are cards that can be loaded with a specific amount of money and used to make purchases or withdraw cash at ATMs. These cards are not linked to a bank account, but rather are funded with a predetermined amount of money. They can be used anywhere that accepts debit card payments.

• Electronic benefit transfer (EBT): Electronic benefit transfer (EBT) is a system to benefit the government to distribute benefits such as food assistance or unemployment benefits. EBT uses a debit card that can be used to make purchases or withdraw cash. Users can access their benefits by using their EBT card at participating retailers or ATMs. EBT is intended to provide a more convenient and secure way for beneficiaries to receive and use their benefits.

In the existing mobile payment system, the model employed is a client-server-client based architecture. It is normally composed of Customer (the one who wants to buy), Issuer (Bank or Financial supporter) and Merchant (the one who wants to sell). In this model the client makes a request to the payment gateway to deduct money from the Customer’s bank account. The Merchant makes a money claim request to transfer money to his bank account. This model involves a third-party intervention and without a stable internet the transaction fails.[3]

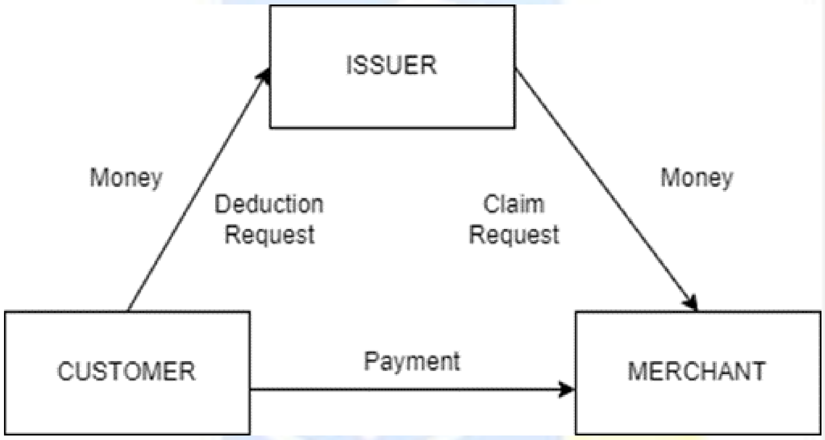

Fig.1 Client-server-client model

IV. PROPOSED MODEL AND ARCHITECTURE

The innovative thought of this process is to create an anti-vulnerable payment system using the wear os wristband. This system is developed on two technologies such that they are a combo of biometric fingerprint sensor and near field communication technology. Smartwatches are existing at present but it on;y comes with a biometric fingerprint security system or comes with NFC automation. So, this system objective is to merge these both automated technologies to output the final product by contemplating security parameters and user friendly parameters. The wristband is produced using the biometric sensor installed and NFC hardware which is responsible for the transfer of confidential card data between wrist band and reader. While the operator touches the wrist band against the reader/POS while performing a transaction , first the sensor of biometric modules receives a power source from the reader and authenticates the user’s fingerprints against the saved fingerprints. If the fingerprint matches successfully then wrist band switches orelse the transaction process fails. The fingerprint utilizes light energy and capacitors to produce the image of ridges and valleys on fingers. It creates a virtual copy of the fingerprint on the display. Electric power source is used to produce virtual fingerprints. After all details are stored in the memory,every time your fingerprint is scanned, then it will authenticate the identity against saved data. To develop a more appropriate and accurate image of fingerprints, the scanner requests to take multiple prints from the same finger. The further task is to activate the passive NFC tag inside the wrist band. The NFC tag in the wrist band takes the power source from the reader. The key security feature refers if the fingerprint match stops then the NFC tag inside the wrist band won't be activated. It states the only authorized member needs to finish the transaction process. This also aids in the prevention of unsecured transactions by stealing the card.

The NFC tag is placed in wrist band to make a communication channel between the wrist band and the reader.[1]

(1) Flowchart and Working

The process to run this project is discussed below. Every process depends on the further process. Failing at a certain process may affect the entire system. The benefit of this transaction system is that the money will be deducted from the user's account only when the fingerprint authorization process proceeds successfully. Detailed process is discussed below.

The below flowchart Fig. 2 discussed the actual working of the project.

Initiate the payment process by tapping on the wrist band. Smartwatch with the aid of power supply from the reader and turns on the fingerprint. Scan the finger by keeping your finger on the fingerprint sensor placed on the wrist band. The fingerprint sensor will collect the fingerprints and match them with saved fingerprints.Collected data of the fingerprints are saved in the wrist band during issuing of the wrist band from the bank. If fingerprint authentication is successful then only the payment process begins or else the process stops there.If matches successfully then the transaction completes successfully. If payment fails then this process checks for user interrupts like finger not placed correctly, the wrong finger detected, finger covered with something unable to scan properly etc. If a wrist band user interrupt is there then deploy the transaction in this stage. To complete the payment transaction, the wrist band user can initiate again from the start. Completion of the process. Termination of the payment.[1]

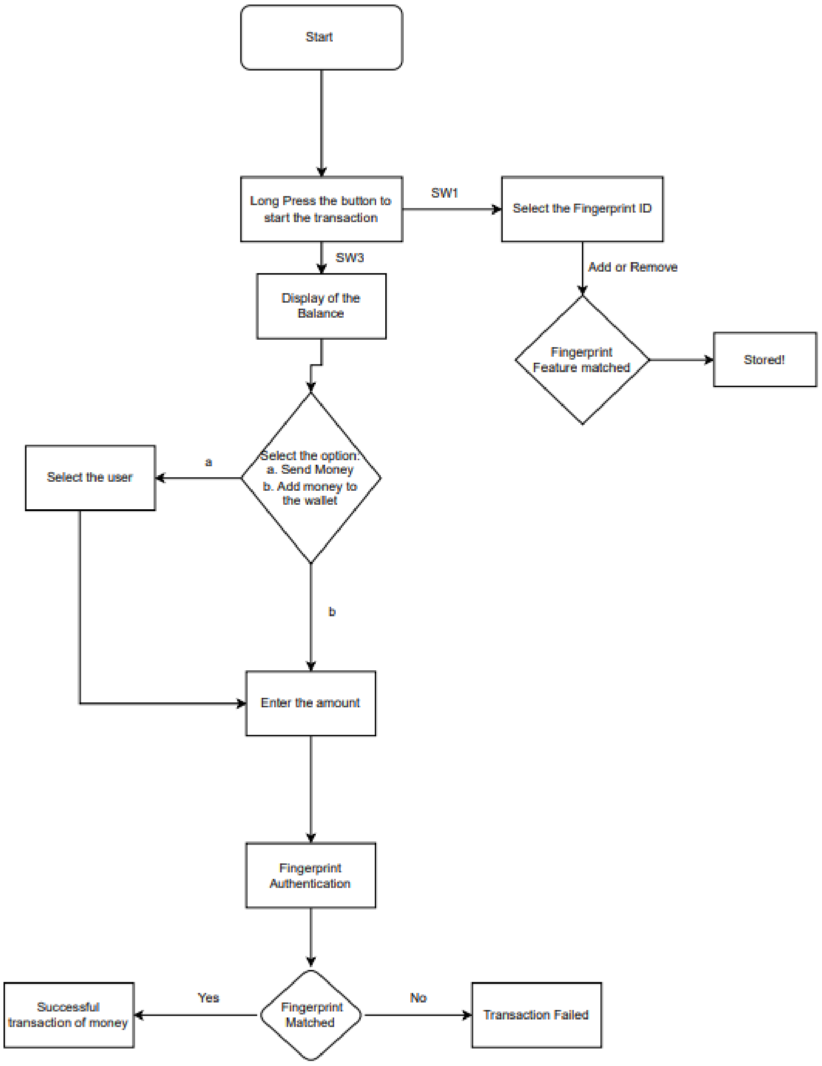
Start
Long Press the button to start the transaction
SW1
Select the Fingerprint ID
SW3
Add or Remove
Display of the Balance
Fingerprint Feature matched
Stored!
Select the user
a
Select the option: a. Send Money b. Add money to the wallet
b
Enter the amount
Fingerprint Authentication
Yes
No
Successful transaction of money
Fingerprint Matched
Transaction Failed

Figure-2 Flow chart

COMPARISON STUDY

Title of the paper with citation	Methodology	Advantages	Disadvantages
Contactless Transaction Using Wearable Ring With Biometric Fingerprint Security[1]	Authentication using Fingerprint	User authentication	No NFC, No user interface
A survey on wearable technology:History,State-of-the-art and current challenges [28]	Wireless Communication	Study about wireless communication, wearables	No authentication
Designing A Wristband That Enables Money Transfer Using Bluetooth [3]	Authentication using Fingerprint, Bluetooth	User authentication	No NFC
WatchAuth: User Authentication and Intent Recognition in Mobile Payments using a Smartwatch [4]	Payment through NFC	Payment through NFC	No fingerprint authentication

Table 1-Comparison between different papers

V.CONCLUSIONS

The objective of this paper is to address all the difficulties that are there in the current wristband payment device. This can be done by the use of wearable devices such as wrist bands. The wear os band will be fixed with NFC tag, crypto processor and fingerprint scanner. The benefit of this is that the authentication will be done before the transaction process will be initiated. The payment process will consume around 1.2 s to complete. Future work of Contactless payment Transaction which aids wear os band with Biometric Fingerprint Scanner is the actual implementation. This device will bring innovation in the payment industry because of having so many benefits over the existing one. This smartcard payment overcomes the challenges in the existing product in a more secure way of payment. The implementation stage is a combination of the hardware resource gathering, development and testing of the hardware and software. The wearable band is secure as per user's view as it follows standard security protocols followed by EMV and the band is based on the government's rules and regulations in the banking sector. This will be the new device in the transaction industry. Existing bands in the industry are able to do transactions but fingerprint scanning security systems aren't assembled on the band. Few upcoming bands do have fingerprint scanners but it is limited to one-time authentication only. So, this objective differs from present inventories and devices. Smartwatches are existing but it comes with only biometric fingerprint security or comes with only NFC technology. So, this system objective is to merge these both automated technologies to output the final product by contemplating security parameters and user friendly parameters.

VI.REFERENCES

[1]Amit Magdum, E. Sivaraman, and Prasad B. Honnavalli Contactless Transaction Using Wearable Ring with Biometric Fingerprint Security Feature

[2] Yashvi Jain *1 , Vipul Jain *2 , Md. Rizwan Khan Digital Payments

[3] Peter Rulić, Bojan Kotnik, Saša Klampfer, Amor Chowdhury Touch-and-Go Mobile Payment System

[4]Y. Rakesh Kumar1 , Voohitha Bojja2 , Vennapusa Bhavika Reddy3 , Batikiri Anuradha4 , Bhavya Velichety5 Designing A Wristband That Enables Money Transfer Using Bluetooth

[5]Jack Sturgess, Simon Eberz, Ivo Sluganovic, and Ivan Martinovic

WatchAuth: User Authentication and Intent Recognition in Mobile Payments using a Smartwatch.

[6]Jack Sturgess, Simon Eberz, Ivo Sluganovic, and Ivan Martinovic(2) WatchAuth: User Authentication and Intent Recognition in Mobile Payments using a Smartwatch

[7] Postrel RD, Haven KR, Empson EH, Fang CC (2017) Point of sale device. United States Patent, Postrel at al. Patent Number: 6,003,008. 19

[8] Breed DS, Johnson WC, DuVall WE (2019) Smartcard. United States Patent, Intelligent Technologies International, Inc. Patent Number: US10,438,106B2

[9] Dory JR, Hanes DH, Dowdy JG (2018) Near field communication (NFC) data transfer. United States Patent, Dory et al. Patent No.: US10,021,727B2

[10] Smart Card Alliance The what, who and why of contactless payments. A Smart Card Alliance Contactless Payments Council White Paper, Publication Number: CPC-06002

[11] Spencer CA (2019) RFID /NFC functionality for portable electronic devices. United States Patent, Spencer, II. Patent No.: US10, 387870B2

[12] Kulkarni G, Bangalore (IN) (2012) Near field communication device. United States Patent, Patent No US9, 087.227B2

[13] Francis L (2018) NFC-enabled devices for performing secure contactless transactions and using HCE. United States Patent Application Publication, Francis, Pub. No.: US2018/0165673A1

[14]Luo J-N, Yang M-H (2019) EMV-compatible offline mobile payment protocol with mutual authentication.Sensors 19:4611 103390/s19214611

[15] Fisher M, Oakland, CA(US); Rathin Guha, Alameda, CA(US) (2016) Mobile Communication Device Near Field Communication (NFC) transactions. United states Patent, Patent No US9,378.493B2

[16] Kienzle W, Hinckley KP (2017) Smart ring. United States Patent Kienzle et al, Patent No.: US 9,582,076 B2

[17] M/Chip Advance Card Application Specification Payment & Data Storage Version 1.2.1—August 2016

[18] Yousefpor M, Busat J-M, Lyon BB (2018) Fingerprint sensor in an electronic device. United States Patent, Yousefporetal. Patent No.: US9,984,270B2

[19]Lin W-C, Hsiao C-J, Tseng S-H (2019) Fingerprint identification unit. United States Patent, Lin etal. Patent No.: US10,430,637B2

[20] Salle VDJ, De Loi T (2016) Contact smart card. United States Patent, Salle et al. PatentNo.:US9.251,457B2

[21]Wu X, Chen Y, Li S (2018) Contactless smart card experiments in a cybersecurity course. IEEE Frontiers in Education Conference (FIE)

[22] Tunstall M, Mayes K, Markantonakis K (2017) Smart card security. https://www.researchgate. net/publication/226129109

[23] Bennett JN (2016) The smart-chip credit card: a current solution. Economic Research Federal Reserve Bank of St. Louis

[24]Adams NP, Waterloo (CA); Ravi Singh, Toronto (CA); Vincenzo Kazimierz Marcovecchio, Ottawa (CA) (2013)Mobile communications device providing near field communication (NFC) card issuance features and related methods. United states Patent, Patent No US 9,154,903 B2

[25]El Madhoun N, Pujolle G (2016) Security enhancements in EMV protocol for NFC mobile payment in 6 IEEE TrustCom-/BigDataSE/-ISPA

[26]Giese D, Liu K, Sun M, Syed T, Zhang L (2018) Security analysis of near-field communication (NFC) payments. arXiv:1904.10623v1[CS.CR]. 24 Apr 2019–12 Aug 2018.

[27] Dr L.Srinivas Reddy, Nakka Uday Kumar A STUDY ON IMPORTANCE OF CASHLESS TRANSACTIONS IN INDIA.

[28]Aleksandr Ometov [a], Viktoriia Shubina [a e], Lucie Klus [a d], Justyna Skibińska [c a], Salwa Saafi [c a], Pavel Pascacio [d a], Laura Flueratoru [e a], DarwinQuezada Gaibor [d a], Nadezhda Chukhno [b d], OlgaChukhno [b a], Asad Ali [a c], Asma Channa [e b], Ekaterina Svertoka [e c], WaleedBin Qaim [a b], Raúl CasanovaMarqués [c d], Sylvia Holcer [d c], Joaquín TorresSospedra [d], Sven Casteleyn [d], Giuseppe Ruggeri [b], Giuseppe Araniti [b], Radim Burget [c], Jiri Hosek [c], Elena Simona Lohan A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges