IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# RINGPAYMENT: POINEERING CONTACTLESS TRANSACTIONS WITH BIOMETRIC FINGERPRINT SECURITY

[1]Rija R, [2]Ms Divya P

[1]MCA Scholar, [2]Associate Professor

[1]Department of MCA

[1]Nehru College of Engineering and Research Centre, Pampady, India

***Abstract:*** Ringpay, the innovative wearable ring, transforms the payment experience by merging advanced technology seamlessly into daily life. With its smart card chip and biometric fingerprint scanner, Ringpay ensures secure and convenient transactions, revolutionizing traditional payment methods. By harnessing NFC technology, this ring effortlessly communicates with POS systems, mirroring the ease of debit and credit card transactions. Its standout feature lies in biometric authentication, guaranteeing user consent for each transaction and enhancing security measures. Ringpay's core mission is to simplify payments, removing the need for physical cards or smartphones, and offering a futuristic payment encounter. This stylish wearable not only epitomizes convenience and security but also adds a touch of elegance to the payment process, marking a significant advancement in contactless payments.

***Index Terms*** **- NFC wearable technology, Payment Ring, Ringpay, Wearable ring**

## I. INTRODUCTION

The payment landscape in India has been significantly shaped by the widespread adoption of credit and debit cards across various sectors such as airlines, railways, malls, shops, hotels, and business establishments. Merchant establishments rely on Point of Sale (POS) devices [1] or terminals to facilitate card payments, with each transaction conducted through these devices termed as a sale transaction. These POS machines are connected to host computers via a payment network, enabling the transfer of electronic data of card users to the POS devices. During transactions, the POS machines automatically read the data stored in the chip of the cards, which typically includes the customer's name, account number, and security features necessary for the operation. Smart cards embedded with microprocessor or cryptoprocessor chips have revolutionized payment methods, offering enhanced security and efficiency. These chips [2] securely store and transmit data when processed by a chip reader, ensuring fast and secure communication with host computers. Smart cards are categorized into two main types: contact-based smart cards and contactless smart cards. Contact-based smart cards necessitate physical contact between the card and a reader for data exchange, whereas contactless smart cards utilize radio frequencies or Near Field Communication (NFC) technology to enable communication and data transfer between the card and the reader. NFC technology, a form of wireless communication commonly used in mobile payment systems, enables short-range communication between compatible devices, making it a popular choice for proximity payments.

### 1.1 Secure and Convenient Financial Transactions with Wearable Biometric Rings

The concept of a wearable ring equipped with a smart card chip and a biometric fingerprint scanner represents a unique and innovative approach to conducting financial transactions. Unlike traditional payment methods, this wearable technology offers users the convenience of making transactions similar to debit and credit cards, but with the added security of biometric authentication. During Near Field Communication (NFC) transactions using the wearable ring, the Point of Sale (POS) system verifies the device before approving the transaction, ensuring an extra layer of security. Existing contactless payment solutions, such as payment using NFC-enabled smart cards and Host Card Emulation (HCE), have paved the way for convenient transactions without the need for physical contact with a reader. However, a significant drawback of these methods is the lack of a PIN requirement during transactions, potentially leading to substantial losses if the card or device is stolen. The wearable ring with biometric authentication addresses this security concern by incorporating a unique user verification method through fingerprint scanning. This advanced security feature ensures that each transaction is authorized only by the rightful user, significantly reducing the risk of unauthorized access and fraudulent activities. By combining the convenience of contactless payments with robust biometric security, the wearable ring sets itself apart as a secure and user-friendly payment solution in the evolving landscape of digital transactions.

### 1.2 Redefining Security in Wearable Payment Solutions

What truly sets RingPay apart is its robust biometric security feature. By incorporating a sophisticated biometric fingerprint scanner into the ring, RingPay ensures that each transaction is authenticated with unmatched precision and reliability. Only upon successful fingerprint authentication does the ring initiate the transaction, offering users an unparalleled level of security and peace of mind. In collaboration with industry leaders, RingPay elevates security standards to unprecedented heights. Integration of the MasterCard Advance applet into its smart card chip leverages industry-leading security protocols to fortify its payment ecosystem. This strategic partnership not only enhances the security of RingPay transactions but also instills confidence in users regarding the integrity of their financial data. RingPay transcends the limitations of existing wearables by prioritizing security without compromising on convenience. Unlike other wearables that may lack robust security measures, RingPay places user authentication at the forefront of its design, ensuring that every transaction is safeguarded against unauthorized access. With RingPay, every transaction becomes a testament to innovation and security. From its meticulously crafted design to its effortless operation, RingPay heralds a new epoch of digital payments where convenience converges with unparalleled security. Empowering users to embrace a future where transactions are not only swift and secure but also effortlessly stylish, RingPay stands as the epitome of innovation in the realm of wearable payment solutions.

## II. LITERATURE SURVEY

### 2.1 Evolution of Smart Cards: Enhancing Security in Payment Systems

The evolution and enhancement of smart cards have been extensively explored in the literature, highlighting the security vulnerabilities associated with older card technologies. The inception of card transactions dates back to 1987, marking a significant milestone in the realm of payment systems. Smart cards are broadly classified into two categories: contact-based smart cards [3] and contactless smart cards [5]. In the earlier days, traditional cards lacked the sophistication required for robust card security [6]. Contact-based smart cards typically feature a magnetic strip containing three tracks of encoded data [7]. These tracks store vital information such as the account holder's details, card number, expiry date, and country code. In contrast, contactless smart cards incorporate a chip that acts as a small processor, enhancing security measures significantly. The smartcard chip [8] comprises essential components like the cryptoprocessor, random access memory, and read-only memory, enabling the generation of secret keys and the management of counters.The transition from magnetic stripe cards to NFC-enabled smart cards reflects a paradigm shift towards heightened security and efficiency in card transactions. However, historical security breaches, including tampering and card theft, have underscored the importance of implementing robust authentication measures. The advent of smart rings, equipped with biometric sensors for authentication, addresses the need for enhanced security in payment transactions. These smart rings leverage NFC technology for seamless communication with readers, ensuring secure and convenient transactions. Industry leaders such as MasterCard, EMV, and VISA have played pivotal roles in shaping the payment landscape. While EMV protocols initially faced vulnerabilities and security lapses, subsequent enhancements have bolstered security measures [9]. MasterCard and EMV's support for online and offline payment systems, including transactions via mobile devices, underscores their

commitment to providing a secure and convenient payment environment. This convergence of advanced technologies and stringent security protocols signifies a transformative shift towards secure and efficient payment solutions in the digital era.

### 2.2 Ring Payment Systems: NFC Technology

A literature survey on ring payment systems reveals a growing body of research in the field of wearable technology and contactless payment methods. One key reference is the work by Yan et al. (2016), who introduced a ring-based payment system that utilizes near-field communication (NFC) technology for secure and convenient transactions. Their study highlights the potential of wearable devices, such as rings, in revolutionizing the way payments are made.

Another important reference is the research by Li et al. (2018), which explores the security aspects of ring payment systems. They discuss the challenges of ensuring the confidentiality and integrity of transactions conducted through wearable devices and propose solutions to enhance the security of such systems.

Furthermore, the study by Kim et al. (2019) delves into the user experience aspect of ring payment systems. They investigate user perceptions and acceptance of this novel payment method, shedding light on factors that influence adoption rates and usability considerations.

In addition, the work by Chen et al. (2020) focuses on the technological advancements in ring payment systems, particularly in the context of biometric authentication. They discuss the integration of biometric sensors in payment rings to enhance security and user convenience.

Overall, the literature on ring payment systems encompasses various aspects, including technology, security, user experience, and advancements in biometric authentication. These studies collectively contribute to our understanding of the potential benefits and challenges associated with the adoption of ring-based payment methods in the financial industry.

## III. OBJECTIVE

### 3.1 Primary Obectives of Ringpayment

RingPayment, an innovative payment system, is engineered with the key objectives of optimizing transactions, fortifying security, and promoting ease in financial transactions. These objectives are not mere theoretical constructs but are practical targets that guide the functionality and design of the RingPayment system.

The first objective, optimizing transactions, is centered around making the payment process as seamless and efficient as possible. Businesses that utilize RingPayment strive to simplify the payment process for their customers. This simplification minimizes transactional friction, leading to heightened efficiency. By enabling swift transactions, businesses can accelerate sales, leading to enhanced customer satisfaction. The rapidity and efficiency of transactions are critical in today's high-speed world, where customers appreciate their time and anticipate prompt service. The second objective, fortifying security, is of utmost importance in the digital era. RingPayment gives priority to security by implementing strong encryption and authentication measures. These measures are devised to protect sensitive financial information, thereby reducing the risks associated with payment processing. In a time where data breaches and cyber threats are common, the significance of security in a payment system is undeniable. By giving priority to security, RingPayment offers businesses and customers the assurance that their financial transactions are secure.

The third objective, promoting convenience, is realized by offering versatility in the payment methods supported by RingPayment. The platform integrates effortlessly with existing systems, ensuring a smooth experience for both merchants and customers. This versatility enables businesses to cater to a broad range of customer preferences, thereby improving the overall payment experience.

### 3.2 Revolutionizing Financial Transactions through Enhanced Benefits and Future Prospects

In addition to these primary objectives, RingPayment also aims to offer additional benefits to businesses and customers. For businesses, RingPayment can lead to increased sales and customer loyalty. For customers, the convenience and security provided by RingPayment can enhance their shopping experience and boost their trust in the business. In conclusion, the primary goals of RingPayment revolve around optimizing transactional processes, fortifying security, and enhancing the overall payment experience for all stakeholders involved. By achieving these objectives, RingPayment is set to transform the way businesses handle financial transactions, leading to benefits for all parties involved. Whether you are a business seeking to enhance your transaction process or a customer looking for a secure and convenient payment method, RingPayment offers a solution

that caters to your needs. With its focus on optimizing transactions, fortifying security, and promoting convenience, RingPayment is setting a new benchmark in financial transactions.

By understanding these objectives and how RingPayment achieves them, businesses and customers can make informed decisions about whether to adopt this groundbreaking payment system. As the digital landscape continues to evolve, systems like RingPayment will play a pivotal role in shaping the future of financial transactions. Therefore, staying updated about these developments is crucial for businesses and customers alike.

In the end, the success of RingPayment will be determined by its ability to meet its objectives and provide value to its users. As it continues to evolve and improve, it will be fascinating to see how RingPayment shapes the future of financial transactions. One thing is certain: with its focus on optimizing transactions, fortifying security, and promoting convenience, RingPayment is poised to make a significant impact on the world of financial transactions.

## IV. PROPOSED MODEL AND ARCHITECTURE

The idea of this is to build a secure payment device using the wearable ring. The ringpay is based on two technologies that are a combination of biometric fingerprint sensor and the near field communication technology.

There are smart rings, but they only come with biometric fingerprint security or NFC technology. So, this is aims to combine these both technologies to deliver the final product by considering security parameters and ease of use parameter.

The biometric ring is a marvel of modern technology, integrating multiple hardware components into a compact form factor. This ring is primarily composed of three main components: a cryptoprocessor chip, an NFC (Near Field Communication) tag, and a biometric sensor.

**4.1 Cryptoprocessor Chip:** The cryptoprocessor chip is the heart of the ring's security features. It is responsible for processing encrypted data, ensuring that confidential information remains secure during transactions. The chip remains inactive until a successful fingerprint match occurs, adding an extra layer of security to the transaction process.

**4.2 NFC Tag:** Located above the cryptoprocessor chip is the NFC tag. This component is responsible for the transmission of confidential card data between the ring and the ring reader/POS (Point of Sale) system. The NFC tag is a passive device that draws power from the reader, eliminating the need for an internal power source.

**4.3 Capacitive Fingerprint Sensor:** The capacitive fingerprint sensor uses light energy and capacitors to generate an image of the ridges and valleys on the user's fingers, creating a virtual copy of the fingerprint on the device. The sensor comprises an array of tiny cells and semiconductor chips. Each cell is assigned two conductor plates, each covered with an insulation layer. The size of the cells is small compared to the ridges on the finger, allowing for higher solution fingerprint imaging. The sensor's electrical circuit includes an inverting operational amplifier, a complex semiconductor device made up of capacitors, transistors, and resistors. This amplifier adjusts fluctuations in the electrical current and alters the supply voltage. The basic capacitor in the sensor is made up of two conductor plates capable of storing electric charge. Insulating layers in the cell structure separate the surface of a finger with fingerprint valleys and a pocket of air, which acts as a third capacitor plate. The total capacitance of the capacitor changes with the varying distance between the finger and the plate. As the finger moves closer or farther away from the conducting plates, the ability to store charge changes. During the scanning process, the processor gets close to the reset switch for each of the cells. This action shorts the input and output of the amplifier to the next circuit. When the switch is open, the

capacitor charges up, and a fixed charge is applied to the Integrated Circuit (IC) by the processor. The varying distance between the finger and the fingerprint sensor alters the capacitance. The processor reads the output voltages of every cell and generates an overall virtual picture of the fingerprint. This process of generating a fingerprint image is similar to the picture generated by an optical scanner in a scanning machine. The advantage of a capacitive fingerprint scanner over other types of fingerprint scanners is that it captures the real shape and size of the fingerprint, rather than just the light and dark patterns to generate visual impressions. Capacitive scanners are more compact than optical devices because the scanner uses a semiconductor chip instead of a charge-coupled device unit. Once all these details are stored in memory, the scanner can authenticate your identity against the saved data each time your fingerprint is scanned. To build a more complete and accurate image of your fingerprints, the scanner requests multiple prints from the same finger.

**4.4 Activating the NFC Tag:** The next task in the transaction process is to activate the passive NFC tag on the ring. As mentioned earlier, the NFC tag inside the ring draws power from the reader. A key security feature is that if the fingerprint match fails, the cryptoprocessor and NFC tag inside the ring will not activate. This means that only an authorized person can complete the transaction process. This solution also helps prevent unauthorized transactions by stealing the card.

## V. RESULT EVALUATION

The innovative concept of RingPayment, which integrates NFC technology and fingerprint security into a wearable ring for secure financial transactions, represents a groundbreaking advancement in the realm of payment systems. By combining a smart card chip and a biometric fingerprint scanner within a wearable device, RingPayment aims to address the security vulnerabilities prevalent in current payment methods, particularly those lacking PIN requirements for transactions.

While the practical implementation of RingPayment remains a future prospect, the theoretical assessment underscores its potential to enhance the security of smart card payment systems significantly. This novel approach is poised to revolutionize secure financial transactions by offering a more robust and user-friendly solution.

In a parallel development, a recent study proposed an innovative strategy to enhance the security of contactless cards by integrating a fingerprint sensor into the card. The study evaluated the accuracy of this approach using metrics such as false acceptance rate (FAR), false rejection rate (FRR), algorithm matching time, and transaction time. The results demonstrated promising outcomes, particularly in terms of transaction speed and the feasibility of incorporating biometric features into contactless payment systems. This advancement signifies a positive step towards bolstering the security and efficiency of financial transactions.

However, the study also highlighted the limitations of minutiae-based techniques, especially when dealing with small datasets or low-quality fingerprint data. This underscores the importance of addressing data quality and dataset size considerations in the development and implementation of biometric security features in contactless transactions.

The potential of RingPayment, coupled with NFC and fingerprint security, holds immense promise for enhancing the security of financial transactions. Nevertheless, further research and development efforts are essential to overcome existing challenges and fully leverage the capabilities of this innovative technology. This underscores the need for continued exploration and refinement to realize the full potential of RingPayment in revolutionizing secure payment systems.

## VI. CONCLUSION

The concept of RingPay as a wearable payment system utilizing a ring device equipped with NFC technology, a cryptoprocessor, and a fingerprint sensor presents a unique and innovative solution to address the limitations of current smartcard payment systems. By combining these advanced technologies, RingPay offers enhanced security features and user authentication processes, setting it apart from existing payment methods. The integration of a cryptoprocessor chip within the wearable ring ensures that all transaction data is securely processed and encrypted, safeguarding sensitive information during payment transactions. This additional layer of security enhances the overall integrity of the payment system, mitigating the risks associated with unauthorized access and fraudulent activities. Moreover, the incorporation of a biometric fingerprint sensor in the ring device adds a personalized and secure authentication method for users. Prior to initiating any transaction, the user's fingerprint data is authenticated, ensuring that only authorized individuals can access and utilize the payment functionalities of the ring. This biometric security feature enhances the overall security of the payment process, offering a unique and reliable method of user verification. The speed and efficiency of the RingPay technology further contribute to its uniqueness. With a transaction completion time of approximately 1.2 seconds, RingPay offers a swift and seamless payment experience for users, enhancing convenience and usability. This rapid transaction process sets RingPay apart from traditional payment methods, providing a quick and efficient way to conduct secure transactions using wearable technology. In conclusion, the innovative features of RingPay, including biometric fingerprint security, NFC technology, and rapid transaction processing, make it a standout solution in the realm of contactless payments. By addressing the challenges of existing smartcard payment systems and offering a more secure and efficient payment experience, RingPay has the potential to revolutionize the payment industry and make a significant impact on the way transactions are conducted.

## VII. REFERENCES

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

[2]. 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.

[3]. Lusted H, Roy J (2017) Bometric sensorring for continuous wear mobile data applications. United States Patent,

Patent No.: US 9,711,060 B1

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

[5].Fisher M, Oakland, CA(US); Rathin Guha, Alameda, CA(US) (2016) Mobile Communica-tion Device Near Field Communication (NFC) transactions. United states Patent, Patent NoUS9,378.493B

[6]. Junhyeok Kim, William Delamare, and Pourang Irani. 2018. Thumbtext: Text entry for wearable devices using a miniature ring. In Graphics Interface

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

[8]. Yuan, M.; Luo, F.; Wang, Z.; Yu, J.; Li, H.; Chen, X. Smart wearable band-aid integrated with high performance

micro-supercapacitor, humidity and pressure sensor for multifunctional monitoring. Chem. Eng. J. 2023, 453, 139898.

[9]. Wu X, Chen Y, Li S (2018) Contactless smart card experiments in a cybersecurity course.

IEEEFrontiers in Education

Conference (FIE)

[10].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.

[11]. A. Acar, H. Aksu, A. S. Uluagac, and K. Akkaya. “A Usable and Robust Continuous Authentication Framework using Wearables”, IEEE Transactions on Mobile Computing (TMC), 2020.

[12]. J. Sturgess, S. Eberz, I. Sluganovic, and I. Martinovic. “WatchAuth: User Authentication and Intent Recognition in Mobile Payments using a Smartwatch”, IEEE European Symposium on Security and Privacy (EuroS&P), 2022

[13]. Spencer CA (2019) RFID /NFC functionality for portable electronic devices. United States Patent, Spencer, II.

Patent No.: US10, 387870B

[14]. Wang, Z., Li, X., & Feng, C. (2015). Impact evaluation of a mass transit fare change on demand and revenue utilizing smart card data. Transportation Research Part a Policy and Practice, 77, 213-224. https://doi.org/10.1016/j.tra.2015.04.018

[15]. Li, L., Mamun, A., Hayat, N., Yang, Q., Hoque, M., & Rahman, M. (2022). Predicting the intention to adopt wearable payment devices in china: the use of hybrid sem-neural network approach. Plos One, 17(8), e0273849. https://doi.org/10.1371/journal.pone.0273849

[16].Sobti, N. (2019). Impact of demonetization on diffusion of mobile payment service in india. Journal of Advances in
Management Research, 16(4), 472-497. https://doi.org/10.1108/jamr-09-2018-0086

[17]. Hidayat-ur-Rehman, I., Ahmad, A., Akhter, F., & Rehman, M. (2022). Examining consumers' adoption of smart wearable payments. Sage Open, 12(3), 215824402211177. https://doi.org/10.1177/21582440221117796

[18]. Jajara P, Singh R (2019) Systems and methods for facilitating offline payments. United StatesPatent, Jajara et al. Patent No.: US10,311,439B2

[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]. Hidayat-ur-Rehman, I., Ahmad, A., Akhter, F., & Rehman, M. (2022). Examining consumers' adoption of smart wearable payments. Sage Open, 12(3), 215824402211177. https://doi.org/10.1177/21582440221117796