Enhancing Secure Card Payments Using Dynamic Multi-Factor Authentication: A Code_safe_pay Approach with Time-Based Code Generation

Koppula Naveen Reddy
Department of Computer Science and Enigneering, PIET (*Parul university)*, Vadodara, India.
koppulanaveenreddy09@gmail.com

Gamidi Raveendra
Department of Computer Science and Enigneering, PIET (*Parul university)*, Vadodara, India
ravindragamidi@gmail.com

Lambu Nithin
Department of Computer Science and Enigneering, PIET (*Parul university)*, Vadodara, India
nithinnani.lambu@gmail.com

Boda Abhinav Reddy
Department of Computer Science and Enigneering, PIET (*Parul university)*, Vadodara, India
abhinavreddy15996@gmail.com

Dr. Mukesh Kumar
Department of Computer Science and Enigneering, PIET (*Parul university)*, Vadodara, India
mukesh.manit86@gmail.com

Daxa Vekariya
Department of Computer Science and Enigneering, PIET (*Parul university)*, Vadodara, India.
daxa.vekariya18436@paruluniversity.ac.in

Abstract — Project "Code Safe" is designed to increase the dependability and security of software through strong security measures, as well as sticking to coding guidelines. In today's digital world that is characterized by data breaches and cyber threats, the safety of sensitive data and protection against unauthorized entry have become very necessary. The project aims to provide a secure environment for software applications by including encryption, access control, and secure authentication mechanisms. The project ensures that any confidential information is kept safe from unauthorized tampering or access through the use of robust encryption algorithms. Access control mechanisms are also in place to regulate user permissions and restrict access to specific functionalities and data, thus ensuring that only authorized persons can interact with the application. To this extent, multi-factor authentication secure access mechanisms would be integrated into authenticate user identity; hence preventing illegal entries to the system. To this extent also, it marks the significance that the software project places on high-quality maintainability of software codes. As indicated, this increases the general quality of a base of the developed software codes towards industry coding and best standards of practice. In addition, this involves modular designing principles, routine code reviews, and automated testing frameworks for identification and handling of software defects thereby improving the reliability and stability of an application. "Code Safe" is an iteration-based development process that includes continuous security assessments as well as updates throughout the software development lifecycle. By keeping on the latest trends and technologies that evolve in terms of security, this project could be able to integrate cutting edge security features within its application; hence, resiliency toward current threats could be ensured. Finally, "Code Safe" aims at ensuring secure platforms for different types of software such as web services, mobile applications or desktop software. The project tries to inspire confidence in end-users that their data and interactions are safeguarded through a robust security framework and adherence to coding best practices.

Keywords— Security Measures, Encryption, Secure Authentication, Multi-Factor Authentication, Cyber Threats

Introduction

Online payment transaction in the digital era is experiencing an increased occurrence due to cyber-attacks and frauds that are targeted at sensitive financial information. This is because; we have experienced tremendous growth in internet usage around the globe. Therefore, this report intends to present a comprehensive review about project which will include its objectives, implementation, challenges faced, and future prospects. In other words, aims to ensure secure and reliable payment processing by preventing unauthorized access or fraud on confidential financial information through the integration of dynamic code generation and multi-factor authentication mechanisms. Therefore, today's modern society increasingly relies on online banking services where electronic money transfers are conducted by the banks as well as through different types of e-payment systems connected bile phones like SMS-banking. Consequently, this report contains a summary of the project which will discuss its objectives, implementation process, encountered difficulties and future expectations. Furthermore, it also aims at achieving secure transaction [1] initiation through deployment of dynamic code generation' s and multi-factor authentication features in its model which safeguards private financial data from hackers or phishers. In existing complex market conditions, companies must take into account many different factors to succeed in business. For example; through mobile phones using SMS as well as other different types of e-payment systems like those used by banks for electronic money transfer are some ways that people use when accessing internet banking services nowadays. Thus, this paper is meant to outline the project in terms of its goals which it aimed for while executing with problems encountered along the way, and possible remedies. Similarly vital is ensuring transaction security so they can enable their users to transfer funds safely with the help of dynamic code generation' s and multi-factor authentication integrated into their system, protecting personal financial details from hacking.

Achieving this objective entails numerous challenges faced by the consumer when wanting to make a payment for good or services on-line particularly as it pertains to fraudulent transaction risk. Consequently, this paper intends to outline an exhaustive outline of a project including objectives implemented challenges faced with its future prospect. Besides, the organizations have to ensure safe payment initiation by including dynamic code generation features and multi-factor authentication systems in their system for human transactions on the Internet[2].

Literature Review

[1]. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. *Cryptography* **2018**

[2]. Ali Hameed Yassir Mohammed1, Rudzidatul Akmam Dziyauddin2, Liza Abdul Latiff (IJACSA) International Journal of Advanced Computer Science and Applications.

[3]. Khan, H.U., Sohail, M., Nazir, S. et al. Role of authentication factors in Fin-tech mobile transaction security. J Big Data 10, 138 (2023).

[4]. Huster, S., Ströbele, J., Ruf, J., Kropf, T., Rosenstiel, W. (2017). Using Robustness Testing to Handle Incomplete Verification Results When Combining Verification and Testing Techniques. In: Yevtushenko, N., Cavalli, A., Yenigün, H. (eds) Testing Software and Systems. ICTSS 2017. Lecture Notes in Computer Science(), vol 10533. Springe

[5]. Charles S Lubobya, Department of Electrical and Electronic Engineering, University of Zambia.

Role of authentication factors in Fin-tech mobile transaction security (08 September 2023) Author: Habib Ullah Khan Authentication methods limit how much control is possible before an account can be used. While authentication factors enhance security compared to passwords, financial transactions face risks as cybercrime creates more chances for fraud. The main problem for businesses is user authentication for mobile transactions, which can help protect against fraud. The mechanisms and technologies identified in earlier research highlight identity confirmation before conducting any financial transaction to assist with user authentication[3].

Multiple Factor Authentication as a Security Measure in Credit Card Fraud Authors: Himanshu Gupta. Published in: 2020 Cybercrime has been around since 1820, but it gained its force around 2000. With the rise in cybercrimes, there is a need for cybersecurity to protect organizations, protect their reputation, and safeguard the privacy and sensitive information of the users. Cybercrime victims have severe penalties like data loss, privacy breach, and theft of money. This paper is on credit/debit card fraud and how multi-factor authentication is an effective security measure to combat this crime.[4]

ANovel Robust Geolocation-Based Multi-Factor Authentication Method for Securing ATM Payment Transactions (2023) Authors: Abdullah Alabdulatif, Rohan Samarasinghe, and Navod Neranjan Thilakarathne Credit and debit cards are highly used today as a payment medium. They give advantages such as convenience, security, and protection against fraud compared to cash. However, the risks associated Credit/debit cards and payment systems have made financial houses alert to their security. Moreover, the increasing payments transactions in electronic form caused frauds and cybercrime, and enormous financial losses for the business and individuals. Therefore, there is a need to have all reliable strong security measures to protect the electronic payment systems. This research proposes a novel approach for electronic payment authentication against fraud at the ATM level using geolocation combined with other attributes. The device's location confirms that the user of the phone is indeed the owner of the card. Besides, this study provides a mechanism to make easy management of transaction ownership such as turning on or off the authentication, blocking the lost or stolen cards, and setting limits for withdrawals.

Biometric multi-factor authentication: On the usability of the Finger PIN scheme (10 November 2022) Authors: Anudeep Vurity, Sumanth Sai Sriram, Venkata Vamsi Ram Patibandla. Fingerprint authentication has gained popularity due to its superiority over passwords in fields such as law enforcement and immigration. It is effective and easy to use, but there are some issues that may prevent its widespread use. Unique to every person and once compromised cannot be replaced: that makes finger printing a risk for biometric authentication. So we developed a multi-factoric authentication system called Finger PIN which combines different types of authentication factors, such as fingerprints, into a personal identification number; to use Finger PIN the user has to provide fingerprints corresponding to the digits of his PIN; this mapping between digits and fingers is secret and predefined. Our initial assessment shows that the system can withstand the compromise of one or more fingerprints[5]

Using Robustness Testing to Handle Incomplete Verification Results When Combining Verification and Testing Techniques (15 September 2017) Authors: Jonas Str¨ obele, J¨ urgen Ruf, and Wolfgang Rosenstiel For complex software systems, verification involves using formal and dynamic techniques. Formal verification aims to cover all possible inputs and code paths, but it may fall short in complex systems. Dynamic testing can be applied to any software and is used to supplement incomplete formal verification results by testing unverified parts. However, this approach does not take into account the fact that testing only shows the presence of errors and not their absence. Errors which go undetected may create problems in the vulnerable parts of the code

Adaptive Center-Weighted Oversampling for Class Imbalance in Software Defect Prediction (2018) Qi Zha, Xuefeng Yan,Yong Zhou Predicting defects helps ensure the software is of quality. Class imbalance, where a few types of defects are very rare, adversely affects the defect prediction model accuracy. For overcoming this issue, a new technique called Adaptive Center-Weighted Oversampling, or ACWO, has recently been proposed. ACWO adapts the oversampling process for each rare defect type by finding appropriate neighbors and neighborhood sizes. For minority class examples, we determine the adaptive center within its neighborhood. Using this center, neighbors, and the minority class sample, we generate synthetic samples. We then oversample each minority class sample based on assigned weights. These weights are determined by neighborhood

sizes and Euclidean distances to the center. Finally, we build a software defect prediction model using the ACWO algorithm with stacked denoising auto-encoder neural networks[6]

The Quest for Security in Mobile Ad Hoc Networks Authors: Jean-Pierre Hubau, Srdan Capk Research on mobile ad hoc networks has mostly concentrated on routing, with security being less of a priority. This research examines security vulnerabilities in mobile ad hoc networks, including risks to both basic and security mechanisms. Our suggested solution to protect security mechanisms is then presented. The solution is unique because it's decentralized and each node plays the same role.

Multi-Factor Authentication (MFA) Adoption Skyrockets, Offering Stronger Security and Improved User Experience (2023) Authors:Wilkie Joissaint Recent data from Okta, a leading identity management company, shows that Multi-Factor Authentication (MFA) is being used more than ever. Since 2020, the number of people using MFA has almost doubled. This means that companies are taking security more seriously while also making it easier and faster for people to use their online accounts.

A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications (2021) By: ALI GUMA, Mussa Dida,Anael Sam. With smartphones and financial technology, mobile money has become widely adopted in developing countries to enable finance access. Most mobile money systems in the developing countries implement two-factor authentication (2FA) to confirm users' identity. The present 2FA method is very vulnerable to threats since it has a reliance of only a personal identification number and subscriber identity module. This paper is focused on developing a safe and efficient 2FA procedure for mobile money applications. In this procedure, there is heightened security in executing mobile money transfers. It encompasses a PIN with an OTP coupled with a biometric fingerprint that will be the means of identification. For withdrawals, it uses a biometric f ingerprint and a Quick Response (QR) code to confirm the transaction.[7] The security measures include SHA-256 encryption for the PIN and OTP, FIDO for the biometric fingerprint with RSA encryption, and Fernet encryption for the QR code and database records.

Current Multi-factor of Authentication: Approaches, Requirements, Attacks and Challenges (2023) Authors:Ali Hameed Yassir Mohammed and Rudzidatul Akmam Dziyauddin Nowadays, accessing services over the internet has become very common and convenient. Security is essential, and multi-factor authentication (MFA) is highly recommended to address vulnerabilities in single-factor authentication (SFA). There are two main types of MFA approaches: biometric (based on physical characteristics) and non-biometric. However, balancing security and accuracy is a challenging task. Studies on authentication mechanisms have shown mixed results, thus requiring further study. This research paper explores several authentication protocols and their security needs. It offers a thorough analysis and contrast between methods for generating and distributing one-time passwords safely. Additionally, it provides a thorough examination of cancelable biometric technologies, the dangers they face, and the standards they must meet.[7]

I. EXISTING SYSTEM

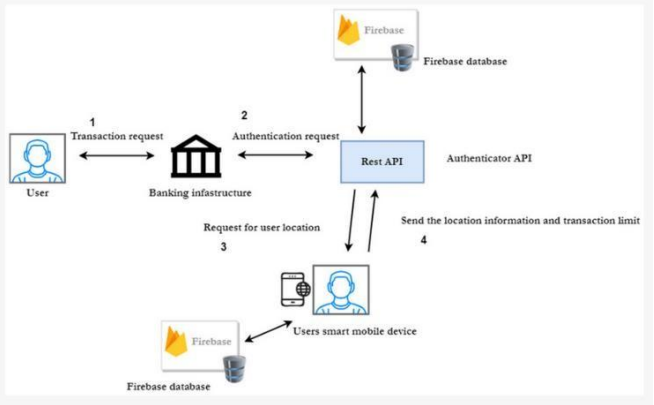


Fig. 1. Overview of the authenticator mobile app

CODE SAFE PAY is an effort to make online payments more secure. It is one of the efforts to make e-commerce more secure. Key objectives are: - Protecting sensitive financial information from unauthorized access and fraud by providing an additional layer of security in payments.- Payment security through dynamic code generation and multi-factor authentication.- Reduction of risks such as identity theft, data breaches, and financial fraud in credit card transactions

Document conventions are rules that make documents look and feel consistent. They ensure that documents are readable and understandable and that they all follow the same basic rules. This makes it easier to compare and contrast different documents and to find the information you need quickly. Versioning and Revisions: Document Version: Display the document's version or revision number prominently. Document Date: Note the date on which the document was prepared or last updated. Language and Tone: Clarity: Use straightforward and clear language to convey the information. Professionalism: Be formal and courteous in the whole document.

The CODE SAFE PAY report points out the theory and practice in secure online payments. It relates to those who need information on dynamic code generation and multi- factor authentication. These improve security when performing transactions. Therefore, it covers the researcher and learner in

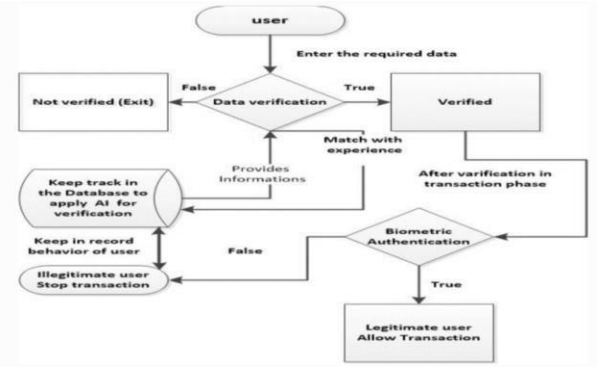


Fig. 2. User verification from use case diagram for transaction

II. Proposed System and Architecture

The CODE SAFE PAY system is made to ensure safety and reliability in online payments. It applies dynamic code generation and multi-factor authentication. Among its very essential parts are those having distinct roles in the payment process. These are the main parts of the system:
Client-side application The client-side application which is used by the customers enables them to initiate and authorize electronic payments.

It can be in the form of a website, phone application or computer program. It provides a convenient way to the customers for using the
payment system. Client-side application that seeks information from customers, initiates payment requests, and communicates with the components in the system at the server end. 4.2.2 Server end Components This is the most critical part of the structure of CODE SAFE PAY. The server end takes responsibility for processing payments, enforcing security, and managing user authentications. Some of the leading components that form part of the architecture are:Payment Processing Server ,External services ,Payment Gateway.

Communication channels-Communicating the data between other modules of software and external systems involves various communication channels. The encryption protocol that is used to protect data transfer during network transmission by the CODE SAFE PAY system includes HTTPS, TLS/SSL, and IPsec. These protocols ensure confidentiality of data by preventing unauthorized access and integrity by protecting against alteration or corruption while in transit

A. Advantages of our Proposed System

- Prevent BruteForce attacks
- Automated keys generated
- Multi factor authentications
- User-Friendly Interface
- Versatility
- Scalability
- Continuous Improvement Potential

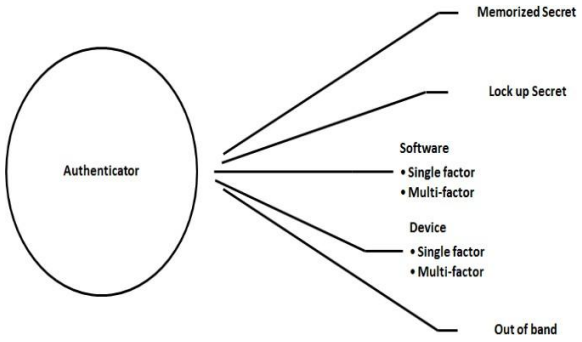


Fig.3. Authenticator's classification.

III. Implementation of Proposed Work

Documentation and Knowledge Sharing Smooth operation and support for CODE SAFE PAY require detailed documentation and knowledge sharing. This section describes documentation strategies, knowledge sharing programs, and training aids developed for administrators, developers, and users. The implementation includes the development of user manuals, API documentation, system architecture diagrams, and knowledge base articles that will make understanding and solving problems for features of CODE SAFE PAY easier.

UI Design CODE SAFE PAY's user interface is simple and easy for all users to pay. The following guide elaborates on the design rules of the UI, its parts, and how people interact with it to make it accessible and reach it for various needs. It is designed differently for various users, such as customers, businesses, and admins, with logical layouts, navigation, and visual cues for seamless and secure online payments.

Fig.4. User Interface of CODE SAFE PAY

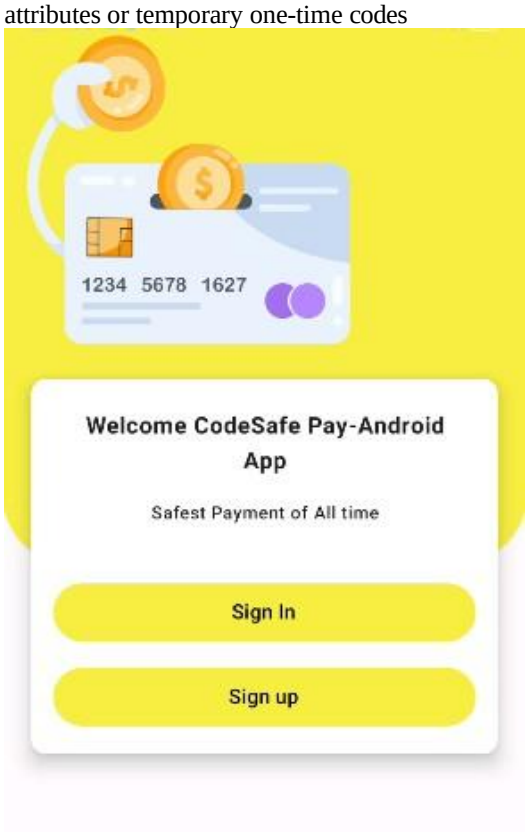
- User Interfaces CODE SAFE PAY has developed several user interfaces (UIs) that provide safe and seamless online payments. These UIs are critical for providing users with simple and straightforward ways to pay while keeping financial information secure and private. Such important UIs in this project include Payment Interface

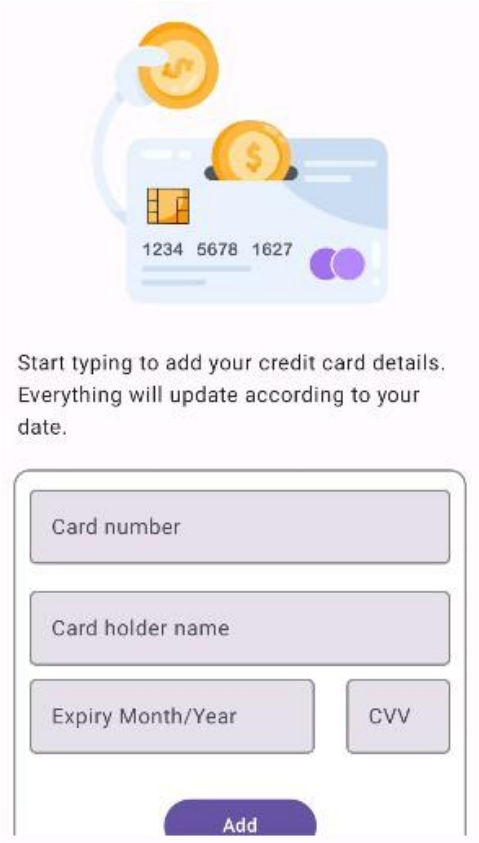
- The payment interface allows users to start and approve online purchases. It usually has things like: Transaction Details: Shows information about the payment you're making, including the amount, who it's going to, and how you're paying

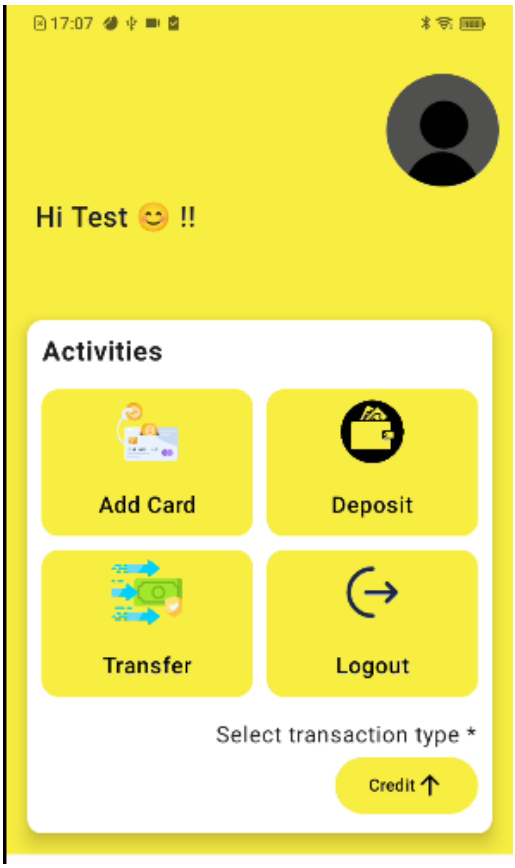
- Dynamic Code Generation: This feature generates unique security codes or tokens; a user must input these to confirm his identity and authorize the action.

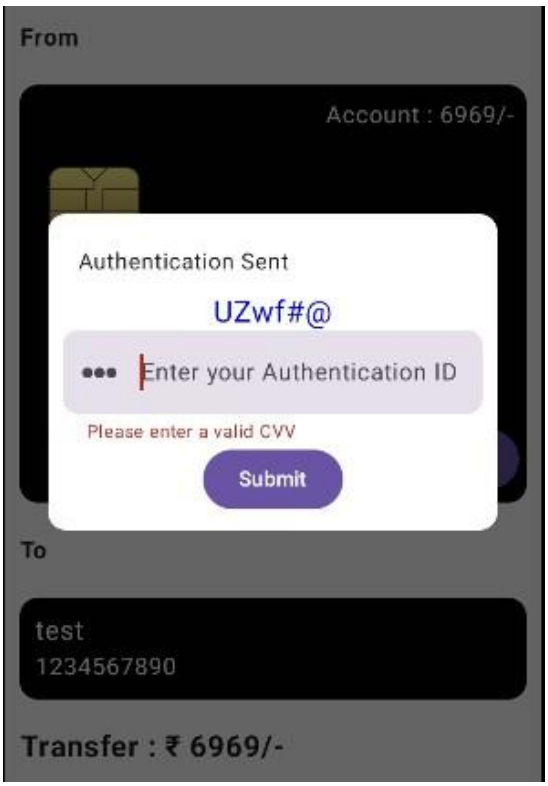
. • MFA- Multiple ways in which a user is authenticated. Methods include: Passwords; Uniquely shaped physical

attributes or temporary one-time codes









. To handle increasing transaction volumes, the CODE SAFE PAY project prioritizes scalability and performance. This involves creating a scalable architecture by leveraging cloud services, using caching mechanisms, implementing load balancing, and optimizing database queries. These strategies aim to enhance system availability and ensure optimal performance under heavy load. essential aspects of the testing and quality assurance processes implemented in the project.

In the CODE SAFE PAY project, testing and quality assurance play a vital role. These activities ensure that the application is reliable, secure, and functions as intended. This section covers the

IV. Results and Modules

The project is composed of several key modules, each with specific roles that contribute to the overall functionality of the proposed system

V. Conclusion

a. In conclusion, CODE SAFE PAY is a breakthrough in online payment security. It offers users a secure, easy-to-use platform for online transactions. Its features include: Dynamic code generation to prevent fraud and ensure secure transactions multi-factor authentication for enhanced security through multiple verification methods Encryption techniques to safeguard financial data Strict access controls to restrict unauthorized access. CODE SAFE PAY prioritizes building a secure payment processing system ensuring scale, high performance, and efficiency in handling large volumes thorough monitoring and continuous improvement to stay abreast of security threats and industry best practices compliance with data privacy regulation in safeguarding user information effective vendor risk management in mitigating external vulnerabilities, ethical considerations, and responsible technology use in fostering privacy and ethics in the digital world.

b.

c. CODE SAFE PAY has ensured considerable safety and dependability for making online payments. This system can avoid illegal accesses and fraudsters using dynamic codes, multi-factor authentication, and encryption techniques to keep all its data secret; therefore, people have been offered better safety as they get absolute security on each online transaction process.

CODE SAFE PAY has greatly enhanced the security of online payments, making it safer and more reliable. It has set a new standard in the industry and helped build consumer confidence. Its robust security features and compliance with industry standards have minimized security risks and vulnerabilities, making online transactions safer. CODE SAFE PAY's influence has not only protected its own platform but has also contributed to a broader, more secure digital environment for all.

References

[1]. Khan, H.U., Sohail, M., Nazir, S. *et al*. Role of authentication factors in Fin-tech mobile transaction security. *J Big Data* **10**, 138 (2023)

[2]. PCI Security Standards Council- This organization sets the standards for secure payment card transactions. Their website contains valuable resources, guidelines, and documentation related to payment card security. Website: https://www.pcisecuritystandards.or

[3]. NIST (National Institute of Standards and Technology)- NIST provides guidelines, standards, and research papers on various topics including cybersecurity and authentication methods.
Website: https://www.nist.gov

[4]. IEEE Xplore Digital Library- IEEE Xplore is a digital library that provides access to research articles, conference papers, and standards related to technology and engineering. You can search for papers on multi-factor authentication and secure payment systems. Website: https://ieeexplore.ieee.org

[5]. Ali Hameed Yassir Mohammed1, Rudzidatul Akmam Dziyauddin2, Liza Abdul Latiff (IJACSA) International Journal of Advanced Computer Science and Applications.

[6]. Khan, H.U., Sohail, M., Nazir, S. et al. Role of authentication factors in Fin-tech mobile transaction security. J Big Data 10, 138 (2023). https://doi.org/10.1186/s40537-023-00807-3

[7]. G. O. Boussi and H. Gupta, "Multiple Factor Authentication as a Security Measure in Credit Card Fraud," *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, 2020, pp. 94-98, doi: 10.1109/ICRITO48877.2020.9197949.
keywords: {Authentication;Credit cards;Computer crime;Organizations;Computer hacking;Law;Credit/debit Card Fraud;Cybercrime;Security Measures;Authentication;Multiple Factor Authentication}, Ghai, P. Kumar, and S. Gupta, "A Deep- Learning-Based Image Forgery Detection Framework for Controlling the Spread of Misinformation," in IEEE Access, vol. 9, pp. 35678-35689, 2021.

[8]. Charles S Lubobya, Department of Electrical and Electronic Engineering, University of Zambia.

[9]. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. *Cryptography* **2018**

[10]. Huster, S., Ströbele, J., Ruf, J., Kropf, T., Rosenstiel, W. (2017). Using Robustness Testing to Handle Incomplete Verification Results When Combining Verification and Testing Techniques. In: Yevtushenko, N., Cavalli, A., Yenigün, H. (eds) Testing Software and Systems. ICTSS 2017. Lecture Notes in Computer Science(), vol 10533. Springe