iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XII **Month of publication:** December 2023

DOI: https://doi.org/10.22214/ijraset.2023.57505

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

National Financial Switch Simulator Using Mobile and Backend SDK

Abhishek Soundalgekar[1], Anand Bhalerao[2], Shruti Deokar[3], Rucha Jadhav[4], Ms. Dipali Kadam[5]
Computer Engineering, PICT, Pune, India

Abstract: ***In the realm of digital finance, the Unified Payments Interface (UPI), managed by the National Payments Corporation of India (NPCI), revolutionizes real-time, boundary less payments between bank accounts. However, Transaction Service Providers (TSPs) encounter challenges in NPCI's testing infrastructure. To resolve this, an independent National Financial Switch (NFS) Simulator for UPI is proposed. This simulator will empower TSPs to conduct autonomous UPI transaction testing, reducing reliance on external resources. By replicating UPI processes, it will facilitate early issue identification, expedite development, and strengthen security. The NFS Simulator's technical implementation involves Android and iOS app creation, NPCI's Common Library integration, and backend simulation, streamlining development and ensuring robustness in the dynamic digital finance landscape.***

Keywords: National Financial Switch, Mobile SDK, Payment Service Providers, App, NPCI, UPI.

I. INTRODUCTION

In the dynamic landscape of digital finance, where security, reliability, and functionality are paramount, the development of robust financial applications is of critical importance. One of the pivotal elements in this ecosystem is the Unified Payments Interface (UPI), a transformative platform revolutionizing digital transactions. Introduced by the National Payments Corporation of India (NPCI), UPI enables seamless real-time payments directly from one bank account to another, regardless of the banks involved. Since its inception, UPI has witnessed unprecedented adoption, becoming the preferred mode of digital payment for millions of users across the country. Its versatility allows for a wide array of transactions, including person-to-person payments, online shopping, bill payments, and more, all accomplished with remarkable speed and security. This surge in UPI's popularity is a testament to its user-friendly interface, instantaneous transaction processing, and robust security features. With the adoption of cutting-edge encryption techniques and two-factor authentication, UPI ensures that sensitive financial information is safeguarded throughout the entire transaction process.

To ensure security, NPCI provides a common library (CL) which is a specification with default implementation. This common library serves as a cornerstone in the UPI ecosystem, offering vital functionalities. It provides essential encryption algorithms, guarantees adherence to stringent security protocols that collectively contribute to the integrity and reliability of UPI transactions. PSP can embed into their UPI app to communicate with NPCI central system to set/reset/change UPI PIN (earlier known as MPIN), balance enquiry and for debit authorization with two factor secured authentication. Common library ensures all sensitive data encrypted with latest technology encryption standards. Employing encryption standards, it ensures that critical information remains shielded from potential threats. These libraries will be available for two major mobile operating systems such as Android and iOS. This inclusivity provides a more integrated and user-friendly experience for consumers across different mobile environments. This ensures that PSPs across a wide spectrum of platforms can benefit from the enhanced functionalities and security measures provided by the library.

However, in the pursuit of enhanced testing and validation, Transaction Service Providers(TSPs) often encounter challenges associated with the reliance on NPCI's testing infrastructure. To address this, the introduction of a simulator proves to be a transformative solution. To achieve these important goals, our project is dedicated to creating a National Financial Switch (NFS) Simulator for UPI. This simulator empowers TSPs with the ability to conduct thorough and comprehensive testing independently, reducing the necessity for extensive coordination and scheduling with NPCI. This simulator is designed to replicate the entire transaction process in a controlled environment, with a specific focus on encrypting and decrypting sensitive user data, such as passwords. Our main objective is to thoroughly test and validate the functionality of our Android app, enhance security measures, and decrease reliance on external libraries.

As a result, TSPs gain a higher degree of flexibility and control over the testing process, ultimately expediting the development and deployment of robust UPI applications.

Moreover, the implementation of this simulator enables TSPs to engage in more extensive and repeated testing without incurring additional fees or charges associated with the use of NPCI's resources.

This level of testing granularity also empowers TSPs to refine their UPI applications with unparalleled precision. Through repeated and in-depth testing, they can identify and rectify potential issues early in the development lifecycle, resulting in a final product that is not only robust and reliable but also finely-tuned to meet the unique demands of their user base. This shift towards self-sufficiency not only streamlines the testing process but also empowers TSPs with the capacity to refine and optimize their UPI applications with unprecedented precision.

Through the NFS Simulator, we aim to establish a controlled environment that mirrors real-world UPI transactions, facilitating rigorous testing procedures. Furthermore, this project aims to decrease our dependence on external tools, which will strengthen our financial application's ability to operate independently and self-sufficiently.

The development of this simulator will not only expedite the development and deployment of UPI applications but also bring about a transformative shift in the way TSPs approach testing and refinement. It bestows them with a newfound level of control, cost-effectiveness, and precision that is essential in navigating the dynamic landscape of digital transactions.

II. LITERATURE REVIEW

In the current scenario of testing of UPI (Unified Payments Interface) applications, transaction service providers (TSPs) require access to a common library provided by the National Payments Corporation of India (NPCI). This library plays a crucial role in the encryption process of sensitive information, such as the UPI PIN (Personal Identification Number) and other pertinent details like in UPI Encryption Process the transactions involve the exchange of sensitive information, including the UPI PIN, which is used to authenticate the transaction. To secure this information, it needs to be encrypted during transmission between the user's device and the UPI infrastructure. The NPCI provides a common library that contains the necessary encryption algorithms and protocols specifically designed for UPI transactions. This library ensures that sensitive data is protected during the transaction process. TSPs rely on the NPCI's common library because it is the authoritative source for encryption methods tailored for UPI. Access to this library is essential for TSPs to implement the proper encryption procedures in their UPI applications. Before deploying their UPI applications in a live environment, TSPs need to thoroughly test the software to ensure it meets security, functionality, and compliance standards. This testing process involves integrating the NPCI's common library into their applications.

[1] The National Payments Corporation of India (NPCI) conceptualized and implemented the Unified Payments Interface (UPI) with the aim of revolutionizing digital payments in the country. UPI enables seamless fund transfers between bank accounts via mobile phones, employing a 1-click 2-factor authentication mechanism for security. The first factor is the user's mobile device, while the second factor involves either an MPIN or biometric verification. While UPI draws on the foundation of IMPS (Immediate Payment Service), it introduces notable distinctions. With a vision to propel India towards a cashless economy, UPI has significantly contributed to the surge in cashless transactions. Despite the user base being a fraction of India's population, UPI recorded an impressive 2.07 billion monthly transactions by October 2020, solidifying its integral role in daily life. This paper delves into UPI's operations, highlights its deviations from conventional cashless transaction methods, explores potential security vulnerabilities, and assesses the efficacy of the UPI BHIM 2.0 update in addressing these concerns.

[2] In the wake of escalating digitization in the banking sector, driven by increased internet accessibility and a surge in digital literacy, the aspiration for a cashless society has gained significant traction. A pivotal milestone in this trajectory materialized with the introduction of the Unified Payment Interface (UPI) by the National Payments Corporation of India (NPCI) in April 2016. UPI has not only wrought a paradigm shift in cashless transactions within India but has also garnered global recognition, solidifying its status as one of the most sophisticated payment systems worldwide. As the prominence of UPI continues its ascent, there arises an imperative to fortify its security apparatus. This research endeavor meticulously scrutinizes the privacy challenges inherent in the extant data flow of UPI models, and proffers discerning methodologies to safeguard the privacy of clientele partaking in transactions via the Unified Payments Interface. This scholarly pursuit contributes substantively to the discourse surrounding the augmentation of security and privacy measures within digital payment systems, in consonance with the dynamic landscape of financial technology.

[3] The Unified Payments Interface (UPI) has emerged as a transformative force in India's digital payment landscape. Developed by the National Payments Corporation of India (NPCI), UPI offers a standardized framework with seamless API specifications, facilitating secure fund transfers and merchant payments. With over a billion transactions monthly, UPI has become a preferred payment solution, revolutionizing the way money moves in India. Contrary to initial skepticism, UPI has garnered significant interest and adoption, dispelling the hypothesis that India might not embrace this technology. Moreover, UPI plays a pivotal role in realizing India's vision of a cashless economy, disproving any doubts regarding its relevance in the broader financial ecosystem. As UPI continues to innovate and expand, it is poised to further catalyze India's digital payment revolution and inspire similar transformations globally.

[4] The project aims to enhance security for UPI PINs by implementing a robust encryption process using AES 256-bit keys, addressing challenges in authentication, authorization, data integrity, and overall security. The approach involves a two-key system comprising a main key responsible for a working key, which, in turn, encrypts the password. Additionally, the paper introduces an improved AES password transmission encryption method, incorporating random number generation as an additional key. This is complemented by the adoption of the RSA transmission encryption process. The system design emphasizes the superiority of 256-bit encryption over 128 bits, with AES utilizing multiple random s-boxes to obscure data placement, thus thwarting potential hackers. The architecture diagram illustrates the interplay between system components, essential for comprehensive comprehension. Notably, the proposed algorithm leverages dynamic multiple random s-boxes to fortify security further. This innovative approach substantially elevates the security posture of UPI PINs, effectively mitigating risks associated with unauthorized access and potential data breaches.
[5] This paper delves into the evolution of mobile banking and payment solutions, particularly focusing on UPI-based applications. In the era of digital transactions, UPI apps have emerged as reliable and secure options, certified by the National Payment Corporation of India (NPCI). The paper acknowledges the potential security risks associated with the mobile app revolution. The study examines UPI-based mobile apps, their architecture, transaction processes, features, and identifies security concerns. It proposes enhancements in authentication and authorization methods to fortify information security. The UPI system is characterized by a simple and secure interface, employing two-factor authentication for transactions. It ensures the confidentiality of user information and leverages advanced mobile device features. Furthermore, the paper addresses the coexistence of UPI and mobile wallets, noting the technological advancements of the latter, albeit with lesser security. The study concludes by suggesting potential improvements such as email alerts, additional authentication fields, and the integration of behavioral attributes and artificial intelligence to augment security measures. These proposed enhancements aim to bolster the security framework of existing UPI applications, particularly in relation to MPIN update transactions and the detection of fraudulent financial transactions.
This research paper [6] discusses data encryption and decryption techniques using the Data Encryption Standard (DES) and Triple Data Encryption Algorithm (3DES) for secure communication. The paper highlights the historical background of DES, its key scheduling, and its weaknesses, leading to the development of 3DES. It also introduces the Advanced Encryption Standard (AES) and Blowfish for comparison. The performance analysis of these encryption algorithms is conducted using different modes, such as Electronic Codebook (ECB) and Cipher Block Chaining (CBC). The results show that 3DES performs better than other algorithms, with AES also being a strong contender. The research provides insights into encryption algorithm efficiency and security.
This paper [7] introduces a new FORTIS algorithm designed to enhance the Key Schedule Algorithm. The Verilog code was executed and the Physical design was generated using Cadence Design Suite. In comparison to the existing Triple-DES, the FORTIS algorithm had a minimal impact on power and area. The power traces for this algorithm were extracted using Chipwhisperer R-Lite (CW1173) and the CW-305 Artix-7 FPGA board. The addition of the Comparator and a versatile shifter to the Key Schedule Algorithm made it more challenging to discern operations from the power trace, resulting in a reduction in PGE values and ultimately enhancing the algorithm's security.
[8] delves into a modified version of the widely recognized RSA-OAEP encryption technique has been incorporated. This modified approach boasts additional benefits, particularly its IND-CCA security, which remains intricately tied to the challenge of RSA. In the context of multi-query scenarios, this method upholds its security. RSA offers robust security for various business applications, and this scheme facilitates the encryption of lengthy messages without the need for hybrid or symmetric encryption, distinguishing it from the AES algorithm.
[9] Ultimately, we can conclude that Blowfish currently exhibits no identified security vulnerabilities, rendering it a commendable standard encryption algorithm. Additionally, it demonstrates remarkable processing efficiency in comparison to alternative encryption methods. It offers versatility in encrypting various image sizes and formats, including .jpg and .bmp. Furthermore, the utilization of Blowfish can lead to enhanced entropy and reduced correlation. When considering AES alongside these attributes, Blowfish's unique strengths become apparent.
[10] Information security is attainable through cryptography, a realm boasting numerous encryption algorithms designed to safeguard sensitive data from potential breaches. While some algorithms have succumbed to cryptanalysis, the strength of any algorithm hinges on the security of its key. Enhanced security can be achieved by encrypting data with multiple keys or utilizing substantial key bit streams (e.g., 128-bit, 256-bit). However, this approach often entails extended computational time, resulting in undesirable delays susceptible to hacking. Leveraging FPGAs can alleviate this concern by providing augmented speed due to their capacity for hardware implementations of encryption algorithms. This improves the overall security posture. When juxtaposed with AES, these characteristics underscore the advantages of FPGA utilization for robust information protection.

Overall, the literature offers a comprehensive overview of UPI, covering its role in revolutionizing digital payments in India, its architectural framework, and widespread adoption and it delves into encryption techniques, highlighting their significance in securing sensitive financial transactions.

III. METHODOLOGY

The implementation of the NFS Simulator necessitates a robust and well-structured methodology to ensure its successful deployment. This section delves into the technical intricacies and design considerations of the system, which includes creating a self-sovereign transaction system, achieving interoperability, establishing permissioned access controls, and leveraging cryptographic methodologies for making secure payments.

A. Creating a Self-Sovereign Transaction System

Establishing a self-sovereign transaction system involves giving users greater control over their financial activities. This is achieved through:

1) *User Registration and Self-Management:* Users can independently register, manage their profiles, and link their preferred financial accounts.
2) *Decentralized Identity:* Implementing decentralized identity solutions, which grant users ownership of their identity and personal information, enhancing privacy and control.
3) *Digital Wallets:* Enabling users to store and manage their financial assets securely within digital wallets, allowing for seamless, self-sovereign transactions.

B. Achieving Interoperability

Interoperability is a key consideration to ensure seamless communication between various components and financial institutions. The methodology encompasses:

1) *Standardized Protocols:* Using industry-standard communication protocols, such as ISO 20022, to enable consistent data exchange between the PSP app, the common library, the backend, and different banks.
2) *API Integration:* Developing standardized APIs that allow for easy integration with diverse banking systems, facilitating the flow of transaction data.
3) *Cross-Platform Compatibility:* Ensuring that the PSP app is compatible with various operating systems and devices to enable widespread usage.

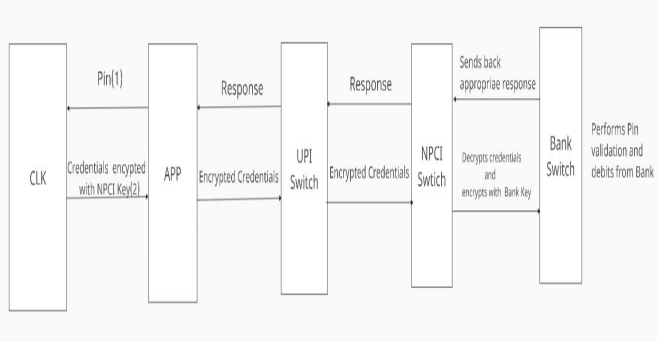


Figure 1 Architecture Diagram

C. Establishing Permissioned Access Controls

To maintain security and privacy, permissioned access controls are essential:

1) *User Role-Based Permissions:* Defining user roles (e.g., admin, regular user) and associated permissions to regulate access to different app features.
2) *Secure API Access:* Restricting access to APIs through authentication and authorization mechanisms, ensuring that only authorized entities can interact with the system.
3) *Data Privacy:* Implementing data privacy controls, such as General Data Protection Regulation (GDPR) compliance, to safeguard user information.

D. Leveraging Cryptographic Methodologies for Making Secure Payments

Secure payments are the cornerstone of the NFS Simulator, and this involves:

1) *Data Encryption:* Implementing strong encryption mechanisms to protect confidential user data, such as MPIN, payer ID, and transaction amounts during transmission and storage.
2) *Digital Signatures:* Utilizing digital signatures to verify the authenticity and integrity of transactions, assuring users of the legitimacy of each payment.
3) *Multi-Factor Authentication:* Employing multi-factor authentication methods to enhance user identity verification and transaction security.

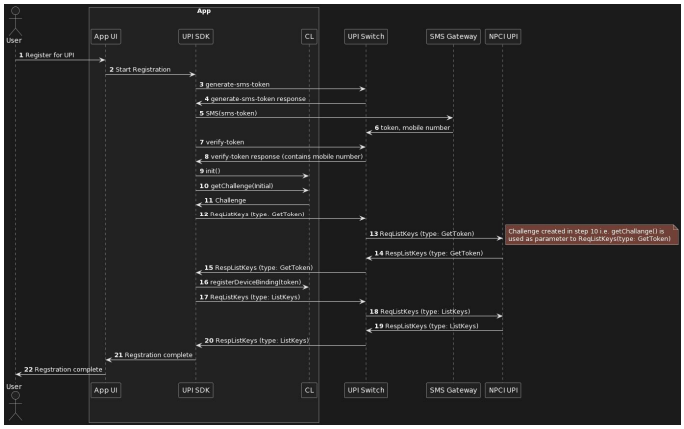


Figure 2 Sequence Diagram

IV. CONCLUSION

The implementation of the NFS Simulator for UPI stands as a landmark progression, significantly reinforcing the development of UPI applications. This innovative solution represents a pivotal advancement by affording Transaction Service Providers (TSPs) an unprecedented level of autonomy, cost-effectiveness, and precision in testing. By furnishing a controlled testing environment, it substantially reduces reliance on external resources, thereby elevating the efficiency and accuracy of UPI application testing.

The introduction of the NFS Simulator signifies a substantial shift toward self-sufficiency, marking a new phase where TSPs gain enhanced control over the testing process, ensuring resilient security and seamless functionality for financial applications within the dynamic digital finance realm. This transformative leap streamlines testing procedures, empowering TSPs to swiftly adapt to the rapidly evolving landscape of financial technology.

By enabling a more self-reliant and controlled testing environment, the NFS Simulator not only represents a significant stride in fortifying digital transaction security but also contributes substantially to fortifying the overall functionality and reliability of UPI applications, heralding a new era of heightened control and efficiency in digital financial services.

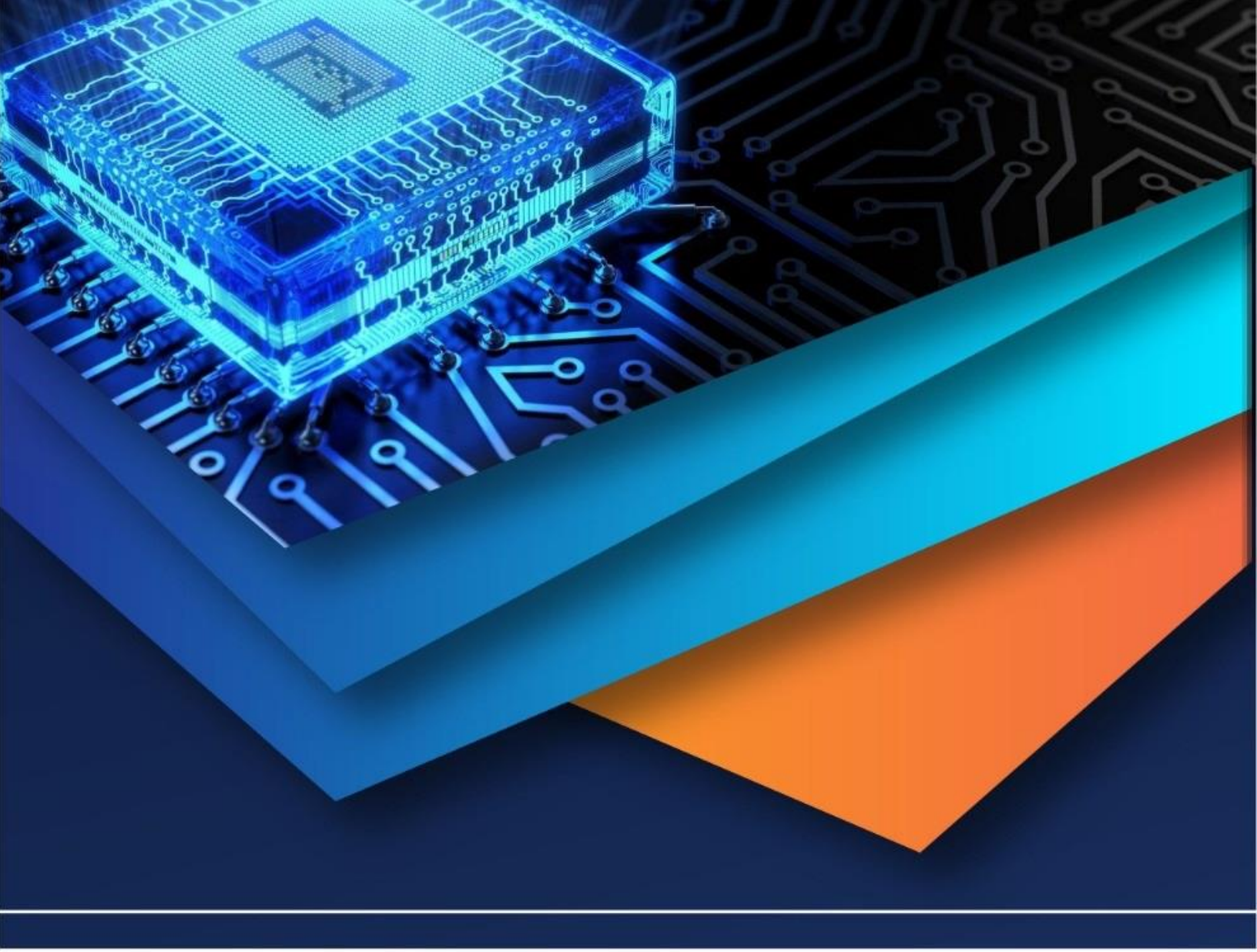
V. ACKNOWLEDGMENT

We would like to express our heartfelt gratitude to our guide, Ms. Dipali Kadam, for her invaluable support, guidance, and mentorship throughout the course of this research. Her expertise, unwavering encouragement, and insightful feedback have been instrumental in shaping the direction and quality of this survey paper. We would also like to extend our thanks to the Computer Department of PICT (Pune Institute of Computer Technology) for providing us with the necessary resources and facilities that were essential for the successful completion of this research project. Their support and contributions have played a pivotal role in our journey to explore the topic national financial switch simulator, UPI and encryption algorithms. We are deeply appreciative of their assistance, and their involvement has been instrumental in our research efforts.

REFERENCES

[1] Y. Madwanna, M. Khadse and B. R. Chandavarkar, "Security Issues of Unified Payments Interface and Challenges: Case Study," 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India, 2021, pp. 150-154, doi: 10.1109/ICSCCC51823.2021.9478078.
[2] S. Vadlamudi and J. Sam, "Unified Payments Interface – Preserving the Data Privacy of Consumers," 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2022, pp. 1-6, doi: 10.1109/ICCR56254.2022.10024689.
[3] Dr. Deepa Baliyan and Dr. Neha Singh. "Unified Payments Interface (UPI): A Digital Transformation in India." IJCRT 11.3 (March 2023): ISSN 2320-2882. Faculty of Commerce, Hindu College, Moradabad, UP, India & Govt. Degree College, Punwarka, Saharanpur, UP, India.

[4] Dr. M. Navaneethakrishnan, Miss. D. Pamila, Miss. M. Mahalakshmi, Miss. B. Praisy. "Encryption and Decryption Of Unified Payment Interface Using Generation Of Multiple Random S-Box With AES Algorithm." International Journal of Advanced Research in Computer Science Engineering and Information Technology 6.3 (Special Issue: 1, Mar 2021): ISSN 2321-3337. St. Joseph College of Engineering, Sriperumbudur, Chennai.
[5] K. K. Lakshmi, H. Gupta and J. Ranjan, "UPI Based Mobile Banking Applications – Security Analysis and Enhancements," 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 2019, pp. 1-6, doi: 10.1109/AICAI.2019.8701396.
[6] Karthik, S., & Muruganandam, A. (2014). Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System. International Journal of Scientific Engineering and Research (IJSER), 2(11), ISSN 2347-3878.
[7] Akshitha Vuppala, R Sai Roshan, Shaik Nawaz, JVR Ravindra,An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm,Procedia Computer Science, Volume 171,2020, Pages 1054-1063,ISSN 1877-0509.
[8] Preetha, M., & Nithya, M. (2013). A Study and Performance Analysis of RSA Algorithm. International Journal of Computer Science and Mobile Computing, 2(6), 126-139. ISSN 2320–088X.
[9] Parihar, Veena & Kulshrestha, Mr. (2016). BLOWFISH ALGORITHM: A DETAILED STUDY. International Journal of Biomaterials Research and Engineering. 3. 2347-4718.
[10] Sawant, A. G., Nitnaware, V. N., Dengale, P., Garud, S., & Gandewar, A. (2019). "TWOFISH Algorithm for Encryption and Decryption." Journal of Emerging Technologies and Innovative Research (JETIR), 6(1), 288. ISSN-2349-5162.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY