Expressive And Deployable Upi Seamless Transaction Using RNN Algorithm

Roselin Lourd J[1], Balaji K[2], Goutham G[3], Jeevaanandhamani M[4], Vijay N[5]

[1]Assistant Professor, Dept of Computer Science and Engineering and Technology

[2, 3, 4, 5]Dept of Computer Science and Engineering and Technology

[1, 2, 3, 4, 5] RAAK College of Engineering and Technology, Puducherry, Pin-605010, India

Abstract*- This In today's world, banking plays an indispensable role among all people. If the banking is user friendly then it would benefit all users. So this situation has forced us to move towards mobile banking system. Emerging technologies have supported people with mobile devices and data connections. Mobile banking applications provide an easy door-step solution for customers. In the current trend of digital and cashless economy, mobile based app solutions are comprehensible and omnipresent, expediting a wide range of banking financial services and non–financial services. UPI is one of the mobile based applications which facilitates online transaction. It is simple and reliable application. Besides positives, there are also some hidden security issues to be resolved. UPI uses PIN to complete the transaction. The PIN entry can be noticed by nearby adversaries. Hence, a direct observation attack based on shoulder surfing becomes a great concern. To cope up with this issue, we come up with the solution of providing high level security after acknowledging that there was a pitfall with the assumption of the previous methods. In our proposed method, we strongly focus on security by proposing a novel approach called Covert Attentional Shoulder Surfing (CASS). In our proposal, we also implement the RNN Classifiers to analyse the behavior characteristics of the user to detect or to resist access by unauthorized people. Our solution or model is also supported by all platforms. It is designed to be used in all platforms (platform Independent) like Android, IOS and other mobile platforms..*

I. INTRODUCTION

UPI Seamless Transaction is an innovative digital payment system . It is a payment system that allows users to send and receive money instantly and securely using their smart phones or computers. The system is powered by Unified Payments Interface (UPI), a real-time payments platform. UPI Seamless Transaction enables users to transfer funds to any bank account, pay bills, and make purchases in a few simple steps. With its simple and secure process, users can instantly make payments and transactions without the need for a card, PIN, or any other physical document. This makes it a great payment solution for both businesses and individuals. Nowadays, the use of mobile devices by people has increased tremendously. A considerable number of people use mobile phones to perform day-to-day tasks .These devices can be used for many tasks, such as making phone calls, web surfing, emailing, gaming, and many other tasks. The current research in this area is focused on the usage of mobile phones to perform payment securely. However, mobile systems face several limitations such as low storage and computation power, due to which they cannot perform heavy encryption operations. Different attacks are reported on mobile devices due to lack of security patches such as spoofing, phishing, malware, and sniffing. In order to effectively design the Mobile payment System, these attack scenarios must be considered for safety and security. Information and communication technology (ICT) is being extensively used all around the world. The traditional face-to-face interaction requirement for payment transactions is avoided, and remote communication is adopted. There is no need for direct contact between a payer and the payee that changes the business environment and leads towards using the Internet to do different transactions. This situation requires electronic money or digital bits; the system resembles traditional payment but uses internet infrastructure and digital data for money transfer. There are many advantages of using e-money, like the client's anonymity or the client's presence is not required during transactions. At the same time, it also has some disadvantages, like compromising of confidentiality, integrity, and availability (CIA).

II. EXISITING WORK

EXISTING SYSTEM :

INTRODUCTION:

Nowadays, security password is the most well-known way to verify a customer to sign in to Computer Systems. However, we all know that conventional text-based security password techniques are susceptible to the shoulder-surfing strike. Through this document we use the phrase "shoulder-surfing" in the following sense: A shoulder-surfing strike includes a customer being shot during his/her sign in.------

EXISTING METHODS :

1. UPI QR Code: UPI QR code allows customers to scan the unique QR code and make payments using their UPI app.

2. UPI ID: UPI ID is a virtual payment address which is linked to your bank account.

3. 3.You can share your UPI ID with the merchant and make payments

4. UPI Payment Apps: You can also make payments using UPI enabled apps like Paytm, Google Pay, PhonePe, etc.UPI is a digital payment system from the National Payments Corporation of India (NPCI). It allows you to transfer money from one bank account to another, without having to enter any sensitive information like debit/credit card details. It is a secure, convenient, and reliable way to make payments. It is supported by all major banks in India and is available through UPI-enabled apps such as Google Pay,PhonePe, BHIM, Paytm, and more. To make a UPI payment, you need transaction method.UPI is a digital payment system from the National Payments Corporation of India (NPCI). It allows you to transfer money from one bank account to another,without having to enter any sensitive information like debit/credit card details. It is a secure, convenient, and reliable way to make payments. It is supported by all major banks in India and is available through UPI-enabled apps such as Google Pay,PhonePe, BHIM, Paytm, and more. To make a UPI payment, you need to enter the recipient's UPI ID and select the bank account you want to send money from. The recipient will then receive a notification of the payment, and you will get a confirmation once the transaction is complete.

Introduction

In the proposed system, the product can be used in commercial transaction such as an interaction between two or more parties in which goods, services or something of value is exchanged for some type of remuneration and personal transactions (Person-to-person payments (P2P) is an online technology that allows customers to transfer funds from their bank account or credit card to another individual's account via the Internet or a mobile phone). Since our solution supports platform independency, it would really benefit a large number of users. This product can be used by all the users who are provided with the bank account. In this solution, we have provided various features for the UPI users so as to benefit them with the seamless transaction. So to assist this, we provide with the following features.

Proposed System Diagram

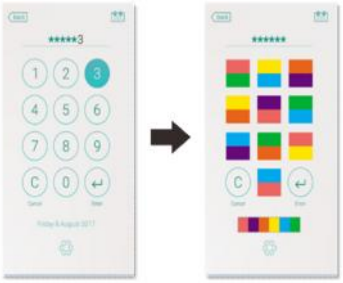


Fig 1.1 Proposed System Diagram

PROPOSED SYSTEM ADVANTAGE:

Very big idea of our proposal which we tend to focus is to prevent Shoulder Surfing (shoulder surfing is a technique used to obtain information such as personal identification numbers, passwords and other confidential data by looking over the user's shoulder) and Unusual Transactions

OVERVIEW:

Behaviour Analyses using RNN classifiers:

The gesture data capturing information reflects the way users interact with their mobile devices. This data is stored and analyzed and if any mismatch is found with the behavioral characteristics, fraudulency is detected and alert message is automatically sent. Recurrent neural network (RNN) classifiers are a type of artificial intelligence (AI) that can be used to analyze user behaviour in a UPI transaction. RNNs are able to capture the temporal dynamics of user behaviour and can be used to detect anomalous behaviour. For example, using an RNN classifier, an AI system can detect when a user’s behaviour is unusually different from their normal pattern. This could be useful in detecting fraud or suspicious behaviour, as it could identify users who are making unusual UPI transactions. Additionally, RNN classifiers can be used to detect patterns in user behaviour, such as when a user is likely to make a UPI transaction or when they are likely to make a large transaction. This could be used to help target marketing campaigns or provide personalized services to users

Fig 1.2 RNN ALGORITHM DIAGRAM

Covert Attentional Shoulder Surfing (CASS):

When a user enters a PIN, there is a chance of direct observation attack by the intruder. So, this becomes a great concern and CASS plays a vital role in preventing the shoulder surfing attack. Covert attentional shoulder surfing is a type of cyber security attack that involves an attacker observing the user's activity without the user's knowledge. The attacker may be able to observe what the user is typing, what information they are accessing, or any other activities they are performing on their computer. This type of attack can be used to gain access to personal or sensitive information, such as passwords, bank account numbers, or other confidential data. It is important to be aware of this type of attack and take measures to protect yourself from it. Common security measures to protect against covert attentional shoulder surfing include using strong passwords, using two-factor authentication, and keeping your computer in a secure location.

PROPOSED SYSTEM TECHNIQUE:

Covert Attentional Shoulder Surfing

RNN CLASSIFIERS

Gesture Data is stored and analyzed and if any mismatch is found with the behavioral characteristics, fraudulency is detected and alert message is automatically sent.

When a user enters a PIN, there is a chance of direct observation attack by the intruder. So this becomes a great concern and CASS plays a vital role in preventing the shoulder surfing attack.

FIG 1.3Covert Attentional Shoulder Surfing (CASS):

PLATFORM INDEPENDENT:

When a product is supported by all the mobile platforms, then it would facilitate most of the users to easily connect with the mobile transaction applications from any platform.

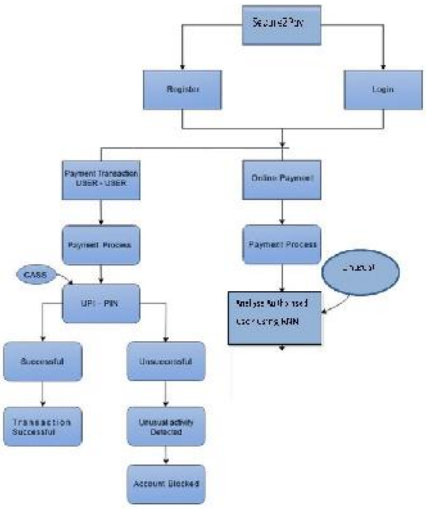


FIG :1.4 PLATFORM INDEPENDENT:

WORKING :

UPI Seamless Transaction is a payment service which enables customers to make payments directly from their bank accounts to merchant accounts without having to enter their banking details every time. The process works in the following way:

1. The customer chooses the merchant and enters the amount to be paid.
2. The merchant then sends a request to the customer's bank for authorization of the payment.
3. The customer's bank then authenticates the payment and sends a confirmation to the merchant.
4. The merchant then sends the confirmation to the customer's bank, which will then debit the amount from the customer's account and credit it to the merchant's account.
5. The customer then receives a notification of the successful transaction

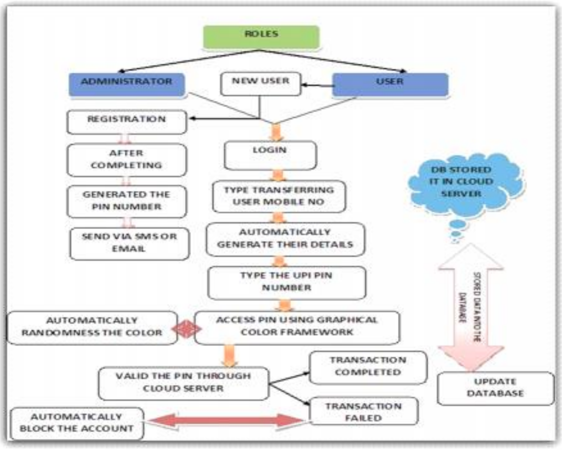
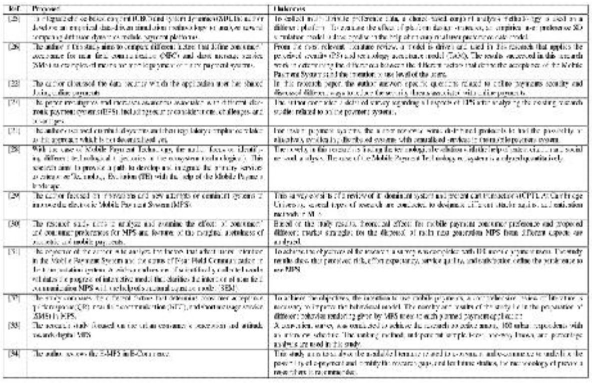

ROLES
ADMINISTRATOR
NEW USER
USER
REGISTRATION
AFTER COMPLETING
GENERATED THE PIN NUMBER
SEND VIA SMS OR EMAIL
LOGIN
TYPE TRANSFERRING USER MOBILE NO
AUTOMATICALLY GENERATE THEIR DETAILS
TYPE THE UPI PIN NUMBER
DB STORED IT IN CLOUD SERVER
STORED DATA INTO THE DATABASE
AUTOMATICALLY RANDOMNESS THE COLOR
ACCESS PIN USING GRAPHICAL COLOR FRAMEWORK
VALID THE PIN THROUGH CLOUD SERVER
TRANSACTION COMPLETED
TRANSACTION FAILED
UPDATE DATABASE
AUTOMATICALLY BLOCK THE ACCOUNT

FIG 1.4 WORKING DIAGRAM

FUNCTIONAL ANALYSIS :

Functional analysis of UPI is the process of understanding how the UPI system works in order to identify potential areas of improvement. The analysis examines the system's functional components, including user interface design, transaction processing, security, customer experience, and other elements. It looks at how the system works and where it could be improved or enhanced.The analysis of UPI is important because it is a key element of the Indian financial system. It is used by millions of people every day to make payments and transfer funds. By understanding how the system works and where it can be improved, it can be used more effectively and efficiently. Functional analysis of UPI can be used to identify weaknesses in the system and to suggest ways to improve the user experience. It can also be used to identify opportunities for innovation and new features. Through this process, the system can be improved to make it more secure and easier to use.

COMPARISON OF SYSTEM FUNCTION:



Ref.	Proposed	Outcomes
[25]	[illegible] system dynamics (SD) [illegible] develop an empirical-based simulation methodology to analyze several competing [illegible] mobile payment platforms.	To collect [illegible] preference data, a choice-based conjoint analysis methodology is used on a different platform. To evaluate the effect of platform design strategies, an empirical user preference SD simulation model is [illegible] with the help of [illegible] preference scale model.
[26]	The author of this study aims to compare different factors that define consumers' acceptance for near field communication (NFC) and short message service (SMS) [illegible] payment systems.	From the most relevant literature review, a model is derived and used in this research that applies the perceived security (PS) and technology acceptance model (TAM). The results succeed in this research work in determining the differences between the different factors that define the acceptance of the Mobile Payment System and the intention to use level of the users.
[22]	The author discussed the data security which the application user has shared [illegible] online payments	In this research paper, the author answers specific questions related to online payments security and discussed different ways to reduce the security threats associated with online payments.
[27]	The paper investigates and mentions [illegible] associated with different electronic payment systems (EPSs) including security considerations, challenges and advantages.	The author concluded a detailed survey regarding all aspects of EPS after analyzing the existing research studies related to online payment systems.
[21]	The author reviewed centralized systems and [illegible] to this approach which is not decentralized yet.	For mobile payment systems, the author [illegible] distributed protocols to find the possibility of [illegible] distributed systems with centralized [illegible] mobile payment system.
[28]	With the case of Mobile Payment Technology, the author focus on identifying different technological trajectories in the ecosystem (technologies). This research aims to provide a path to develop and integrate the [illegible] services as Technology Evolution (TE) with the help of the Mobile Payment landscape.	The novelty in this research is finding the technological solutions with the help of patent citation and social network analysis. The case of the Mobile Payment Technology ecosystem is analyzed quantitatively.
[29]	The author focused on innovations and new attempts or common systems to increase the electronic Mobile Payment System (MPS).	This survey consists of a review of the dominant system and present cart transaction (CPT). At Cambridge University, several types of research are conducted to designate different attacks against authentication methods in MPS.
[30]	The research study aims to analyze and examine the effect of consumers' and consumer preferences for MPS and features of the marginal usefulness of [illegible] and mobile payments.	Based on the study results, theoretical effects for mobile payment consumer preference and proposed different market strategies for the disposal of each next generation MPS from different aspects are analyzed.
[31]	The objective of the author is to analyze the factors that affect users' intention in the Mobile Payment System and the terms of Near Field Communication in the transportation system. [illegible] collected results validates the progress of interactive model that clarifies the intention of near field communication MPS with the help of structural equation model (SEM).	To achieve the objectives of the research a survey was completed with [illegible] mobile payment users. The study results show that perceived risk, effort expectancy, service quality, and satisfaction define the tendencies to use MPS.
[32]	The study compares the different factors that determine consumer acceptance quick response (QR), near field communication (NFC), and short message service (SMS) in MPS.	To achieve the objectives, the intention to use mobile payments, a comprehensive review of literature is necessary to improve the behavioural model. The novelty and results of the study lie in the preparation of different behavior rendering given by MPS users to each planned payment application.
[33]	The research study focused on the urban consumer's perception and attitude towards digital MPS.	A convenient survey was conducted to achieve the research objectives, 100 urban respondents with an interview schedule. The ranking method, independent sample t-test, one-way Anova and percentage analysis are used in this study.
[34]	The author reviews the E-MPS in E-Commerce.	This study aims to analyze the available literature related to e-commerce and e-commerce to underline the [illegible] of e-payment and identify the research gaps, and for future studies, the methodology of preview a research are recommended.

SECURITY ANALYSIS :

1) Confidentiality: Data exchanged among the participants in the framework are encrypted using session keys thereby ensuring confidentiality.

2) Mutual authentication: WPKI is a part of both the device and MPA, which authenticates the entities using certificates. Bank personalizes Payment Applications (PA) in the Customer (C) and Merchant (M), i.e., the Bank shares a separate symmetric key with Customer (C) and Merchant (M), thereby ensuring mutual authentication.

3) Integrity: Intruder will not be able to access or modify the messages. In addition to this, the encrypted message also contains timestamps and nonce, ensuring timeliness and uniqueness properties. So, the intruder cannot modify the messages, thereby ensuring the integrity of the exchanged messages.

4) Accountability: Figure 4 depicts the steps involved in the protocol containing all the entities involved; PG (Payment Gateway) ensures accountability property, collecting evidence from the Bank. The proposed framework implements WPKI. Bank updates the MPA of the Customer and PPA of the POS Over the Air (OTA). PG maintains the Evidence Repository (ER) and Provenance Repository (PR), ensuring accountability property. So, the proposed protocol provides accountability.

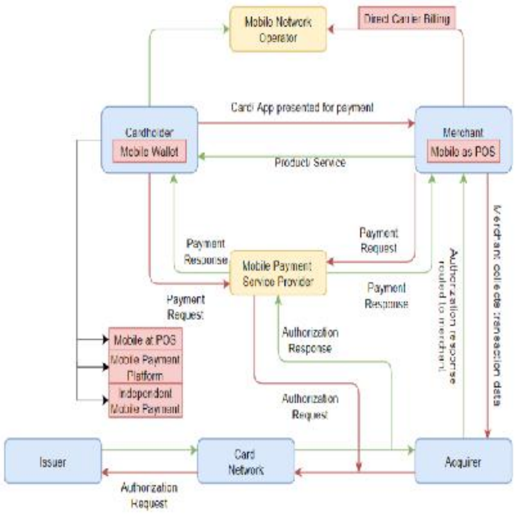
5) Defence in Depth: Our proposed framework incorporates protection in-depth at the SE level and payment application level. WPKI provides application security, and the TLS protocol provides communication security. If the symmetric key is compromised, bank updates the symmetric key in the payment application.

6) Overcomes Heartbleed and ROBOT Vulnerabilities: Heartbleed, and the recent ROBOT [9], [10]. Our proposed mobile payment system uses newer versions of TLS certificates signed by the CA. So our proposed mobile payment system overcomes these vulnerabilities.

7) Fake Terminal and Mobile Application: An intruder cannot reverse engineer MPA and PPA as both (MPA and PPA) overcomes reverse engineering attacks by binary code obfuscation, flow relocation, stripping debugging information, and by encrypting strings and resources in the code, in addition to these Bank enforces Self-Signing Restriction on MPAs and PPAs and codes of these applications is attested by the Bank's private key, so our proposed mobile payment framework overcomes reverse-engineering attacks.

8) Tampering Configuration: The workflow of the con-figuration file in MPA will be modified, so this attack will not be fruitful in our proposed mobile payment system as both MPA and PPA overcome this attack by flow relocation, stripping debugging information, and by encrypting strings and resources in the code, in addition to these Bank enforces Self-Signing Restriction on MPAs and PPAs and codes of these applications is attested by the Bank's private key, so our proposed mobile payment framework overcomes tampering con-figuration attack.

9) RAM Scraping: This attack is also known as memory scraping or memory parsing attack, which retrieves payment information and symmetric keys from the memory of MPA. RAM Scraping or Memory Parsing attack will not be successful from the SE or MPA of either the customer's smartphone or the HSM of the POS as SE and HSM are tamper-resistant. At the same time, MPA and PPA adopt WBC.



ENCRYPTION TECHNOLOGY :

Encryption technology includes Symmetric encryption and public-key encryption.

1) SYMMETRIC KEY ENCRYPTION (SKE)

SKE system uses a common key to encrypt messages, which means both sender and receiver will hold a common key for encryption and decryption. Before transmission of data between both parties, the common key is shared on the secure channel between both entities [51]. Exchanging keys between both entities is important for encryption processes. Short size and weak keys are easily attacked as opposed to longer keys. Symmetric encryption is still commonly used in insecure data communication.

2) PUBLIC-KEY ENCRYPTION (PKE)

PKE system is a type of asymmetric encryption because the same key is not used to encrypt and decrypt the messages. In the PKE system, two different keys are used, called public and private key [51].

3) COMPARISON BETWEEN SKE AND PKE

There are numerous differences between the SKE system and the PKE system. Table 5 presents the comparison of the SKE.

AUTHENTICATION:

Authentication included: Digital signature and certificate authority.

1) DIGITAL SIGNATURE:

Digital signature (DS) is used to verify the origin of the received text and prove whether the received text is without any changes or not. To certify the availability of DS, public keys infrastructure (PKI) is frequently used. It suggests a complete set of security assurance and follows different public key encryption standards for different sectors like online banking, e-banking, e-government, and e-commerce securities [52].

2) CERTIFICATE AUTHORITY

The Certificate Authority (CA) is a trusted organization that publishes and manages network security PKI and credentials for message encryption. As part of the PKI, the CA will use the registry for verification. Users have the right to verify the information in the digital certificate provided by the applicant. Suppose RA (Register Authorities) verifies the applicant’s data and issues a digital certificate. Users are responsible for distributing and revoking certificates in a communication system. Depending on the PKI, upon request, the certificate may contain the holder’s public key, the certificate, the name of the certificate holder, and other information about the holder of the public key [53].

FIREWALL

The firewall can simultaneously protect the system /local network against network-based threats. The firewall allows access to the outside world to the local network. In most scenarios, a firewall is necessary because it is difficult to equip all devices with different security devices. Typically, the firewall is inserted between two networks.

SYSTEM REQUIREMENTS:

HARDWARE SPECIFICATION:

Processor	-	i3 Processor
Speed	-	2.0 GHz
RAM capacity	-	4 GB
Hard Disk	-	500 GB

SOFTWARE SPECIFICATION:

Operating System- Windows '07
Back End - My SQL 5. 0
Front End - PHP MVC Framework

Cloud Hosting - Gsuite Server (Google Cloud)

III. CONCLUSION

Overall, the seamless UPI transaction is a great way to make payments quickly and conveniently. It provides a secure and convenient platform for making transactions, and the transactions can be completed in a few steps. With UPI, users can also send and receive money from any part of India without any additional charges. Additionally, UPI offers an extra layer of security by providing two-factor authentication, which helps to protect against fraud and other malicious activities. With UPI, users can now make payments easily and securely without having to worry about any type of security breaches.

This paper discussed various payment schemes and their usage, technology, and provided security mechanisms. Most payment methods are account-based payment systems, and their main focus is on security, privacy, confidentiality, and authentication. We present an overview and discussed different components of MPS. We presented a detailed survey of the existing MPS structure and its limitations; provided detailed history, development, and deployment of MPS. We discussed different aspects of MPS, including socioeconomic conditions, cost efficiency, diffusion of mobile phones, convenience, new initiatives, heavy restrictions and regulations, limited collaboration, underdeveloped ecosystem, and security problems; the key attributes of MPS, and stakeholder and communication entities roles in MPS form different aspects. We discussed different security mechanisms involved in MPS. We also provide an analysis of the encryption technologies, authentication methods, and firewalls in MPS. All the papers suggest different techniques to provide different security aspects. However, the main point is that keeping in check the CIA triad, each payment should be made with authentication and encryption because the future of MPS depends on its security features.

REFERENCES

[1] S. F. Verkijika, ‘‘An affective response model for understanding the acceptance of mobile payment systems,’’ Electron. Commerce Res. Appl., vol. 39, Jan. 2020, Art. no. 100905.

[2] A. R. Javed, M. O. Beg, M. Asim, T. Baker, and A. H. Al-Bayatti, ‘‘AlphaLogger: Detecting motion-based side-channel attack using smartphone keystrokes,’’ J. Ambient Intell. Humanized Comput., pp. 1–14, Feb. 2020.

[3] S. Cimato, ‘‘Design of an authentication protocol for GSM Javacards,’’ in Proc. Int. Conf. Inf. Secur. Cryptol. Heidelberg, Germany: Springer, 2001, pp. 355–368.

[4] S. Kungpisdan, B. Srinivasan, and P. D. Le, ‘‘A practical framework for mobile set payment,’’ in Proc. Int. ESociety Conf., 2003, pp. 321–328.

[5] L. M. Marvel and C. G. Boncelet, ‘‘Authentication for low power systems,’’ in Proc. Commun. Netw.-Centric Oper., Creating Inf. Force (MILCOM), vol. 1, 2001, pp. 135–138.

[6] Y. Wang, C. Hahn, and K. Sutrave, ‘‘Mobile payment security, threats, and challenges,’’ in Proc. 2nd Int. Conf. Mobile Secure Services (MobiSecServ), Feb. 2016, pp. 1–5.

[7] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. K. Bashir, ‘‘A survey of security and privacy issues in the Internet of Things from the layered context,’’ Trans. Emerg. Telecommun. Technol., p. E3935, Mar. 2020.

[8] C. Iwendi, Z. Jalil, A. R. Javed, T. Reddy G., R. Kaluri, G. Srivastava, and O. Jo, ‘‘KeySplitWatermark: Zero watermarking algorithm for software protection against cyber-attacks,’’ IEEE Access, vol. 8, pp. 72650–72660, 2020.

[9] A. R. Javed, Z. Jalil, S. Atif Moqurrab, S. Abbas, and X. Liu, ‘‘Ensemble AdaBoost classifier for accurate and fast detection of botnet attacks in connected vehicles,’’ Trans. Emerg. Telecommun. Technol., p. E4088,

[10] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava, and M. Abdallah, ‘‘B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain,’’ IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 1214–1229, Apr. 2021.

[11] R. M. Mohammad and H. Y. AbuMansour, ‘‘An intelligent model for trustworthiness evaluation in semantic web applications,’’ in Proc. 8th Int. Conf. Inf. Commun. Syst. (ICICS), Apr. 2017, pp. 362–367.

[12] D. Preuveneers, T. Heyman, Y. Berbers, and W. Joosen, ‘‘Feature-based variability management for scalable enterprise applications: Experiences with an e-payment case,’’ in Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS), Jan. 2016, pp. 5793–5802.

[13] E. Turban, J. Outland, D. King, J. K. Lee, T.-P. Liang, and D. C. Turban, ‘‘Mobile commerce and the Internet of Things,’’ in Electronic Commerce 2018. Cham, Switzerland: Springer, 2018, pp. 205–248.

[14] M. Hubert, M. Blut, C. Brock, C. Backhaus, and T. Eberhardt, ‘‘Acceptance of smartphone-based mobile shopping: Mobile benefits, customer characteristics, perceived risks, and the impact of application context,’’ Psychol. Marketing, vol. 34, no. 2, pp. 175–194, 2017.

[15] W. Stallings, Cryptography and Network Security. Hoboken, NJ, USA: Prentice-Hall, 2005, p. 592.

[16] Securing the Future of Payments Together. Accessed: May 14, 2020. [Online]. Available:

https://www.brighttalk.com/webcast/17380/490469/securing-the-future-of-payments.