IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 6, Ser. 1 (Nov. – Dec. 2025), PP 88-94
www.iosrjournals.org

Comprehensive Security Assessment of NFC-Set Protocol for Financial Applications

Amit Sahu[1], Dr. Dhirendra Kumar Tripathi[2]

[1, 2] Department of Computer Science, Mansarovar Global University, Sehore, M.P.

Abstract

The Secure Electronic Transaction protocol, which makes use of Near Field Communication (NFC-SET), is formally verified in this study's experimental context. Privacy, authentication, integrity, non-repudiation, and replay attack protection are some of the essential security services that will be assessed. The AVISPA tool is popular for analysis because to its robust formal modeling capabilities and several performance verification methodologies. The NFC-SET protocol, which illustrates the interaction between the cardholder, merchant, and payment gateway, is governed by HLPSL. With the help of the OFMC, ATSE, and SATMC backends, eight different situations are reviewed. Attacks that take advantage of a single session, several sessions, or an outsider all fall under this category. The intruder's knowledge is precisely tailored to mimic actual aggressive conduct. None of the tests were compromised, according to the verification findings. It may be concluded that NFC-established successfully accomplishes all of its intended security objectives. Based on these findings, it seems that NFC-SET is a strong and effective solution for NFC-based secure electronic transactions.

Keywords: *Security, Verification, Transactions, Communication, Electronic*

Date of Submission: 07-11-2025 Date of Acceptance: 20-11-2025

I. INTRODUCTION

Secure Electronic Transaction via Near Field Communication (NFC-SET) is a key step in making short-range electronic payment systems safer. The NFC-SET framework builds on the existing Secure Electronic Transaction (SET) protocol by adding the low-power, proximity-based communication features of NFC technology. This link makes contactless payments secure, quick, and easy to use, and it also protects sensitive financial information very well.

NFC-SET's purpose is to protect financial data at every step of a transaction by employing strong cryptographic methods such authentication, secrecy, and integrity controls. The protocol tries to protect against common security threats in wireless communication, such as replay attacks, eavesdropping, impersonation, and unauthorized access. Because NFC-based devices use open radio-frequency channels for transactions, these safety measures are even more important.

In the NFC-SET model, which depends largely on reciprocal authentication, customers, companies, and banks all play essential roles. Before any transaction can happen, digital certificates, secure key exchange protocols, and encryption technologies are utilized to build trust. For these ways to function, everyone participating in the payment process must be real and have permission. Adding non-replay mechanisms and confidentiality assurances to the protocol makes it much harder for others to steal credentials, clone things, or do man-in-the-middle attacks. Automated analytic methods are used to formally check the security of NFC-SET to make sure it is safe. This lets the process be tested in a number of dangerous conditions.

Cellphones have become a big part of many parts of everyday life outside simply talking to people. They are used a lot more than they used to be. People like these gadgets for a lot of reasons, including as getting information, utilizing mobile applications to accomplish work-related tasks, and negotiating business deals. As a result, digital wallets and other currency substitutes have become quite popular. For both financial and non-financial enterprises, mobile payment solutions are becoming necessary for cashless transactions.

Because it is fast, easy to use, and safe, Near Field Communication (NFC) has become a popular alternative to digital payment methods. Payments made via near field communication (NFC) have several advantages, including quick transactions, secure data storage, and the ability to deactivate or erase credentials from a distance if a device is lost or stolen. Payment authorization systems, especially those that employ NFC-Radio Frequency Identification (NFC-RFID) devices, have made a lot of use of NFC technology. Also, near field communication (NFC) is a common feature of mobile wallet applications that enable people pay at stores that accept them. In 2018, near field communication (NFC) technology was present in roughly 64% of smartphones and 53% of the world's POS terminals. This shows how the ecosystem of contactless payments is growing.

DOI: 10.9790/0661-2706018894

The two primary ecosystems that near field communication (NFC)-enabled mobile payment systems work in are the host card emulation (HCE) and the NFC Subscriber Identity Module Secure Element (SIM-SE). The Secure Element (SE) is physically put inside the smartphone's SIM card, thus transactions may still happen with the NFC SIM-SE model even when the internet isn't accessible. The NFC-HCE architecture needs cloud-based Secure Elements to get back and keep important credentials. These Secure Elements need an active internet connection. This reliance makes the system even more vulnerable to attacks since it has to safely communicate credential keys between the cloud and the device.

Even with all these problems, NFC-HCE offers a lot of amazing features. For example, it doesn't need SIM cards with Secure Elements installed. NFC-HCE is more scalable and cost-effective since it is flexible, which makes it more useful in many other fields. Several national mobile payment systems adopted NFC-HCE as a result, especially in places where SIM cards are made that don't work with Secure Element.

Given these challenges and opportunities, this study proposes improving the efficiency and security of NFC-HCE mobile payment systems via the development of an application-based NFC-HCE model. The proposed methodology enables secure NFC transactions, regardless of the presence of a Secure Element in the SIM card. To achieve this, the model moves critical operations to the smartphone and adds Secure Element functionality that is usually found in the NFC SIM-SE ecosystem to the NFC-HCE environment.

The proposed approach allows NFC-enabled smartphones and NFC readers to talk to each other safely using a transaction framework supported by a robust security architecture. The whole idea is made up of two key steps: initialization and transaction execution. The initialization step registers the user and their credit card information with the server so that the phone may be used for near-field communication (NFC) transactions. The device has now checked that the credential info is secure and has been approved. One user may register more than one card.

At this point in the process, the cardholder's mobile device and the POS terminal send important information to each other in a safe and secure way. This stage manages the use of near field communication (NFC) for financial transactions and checks that the data being sent is valid, complete, and private. This study concentrates on the installation and assessment of the transaction component, namely the Application-Level Secure Element (APLSE) mechanism, which facilitates encrypted data transmission and processing between the mobile device and the point-of-sale terminal.

II. REVIEW OF LITERATURE

Ahamad, Shakeel. (2021) The exponential growth of mobile apps has led to an increase in the number of individuals making purchases via these platforms. The current state of mobile payment and commerce research is precarious due to its lack of transport layer protection and susceptibility to reverse-engineering assaults. As a result, MPAs will be the targets of such assaults, which will lead to significant financial losses. To address these issues, we provide a secure design for NFC-based mobile payment systems that uses a defense-in-depth approach. We use a defense-in-depth approach that incorporates protection at the hardware, mobile app, and communication levels. Our suggested protocol, NSPMT, has successfully repelled assaults such as phishing, DOS, DDOS, RAM scraping, and multi-protocol attacks. A mobile payment mechanism has also been validated by us utilizing Scyther and BAN logic. A mobile payment solution that can avoid security flaws like Heartbleed and ROBOT (Return of Bleichenbacher’s Oracle Threat) has been created by our team. Our suggested protocol ensures all security aspects while having much reduced energy, communication, and compute costs compared to earlier research. We have built a POS app, two mobile payment apps, and an Android Studio app using the kotlin language. To protect users' financial information, the applications use Advanced Encryption Standard (AES) with GCM (Galois/Counter Mode) mode and the Elliptic Curve Digital Signature Algorithm (ECDSA).

Thammarat, Chalee (2020) Protocols for near field communication (NFC) have prioritized transmission speed above security features. An authentication request is a message transmitted over the air (OTA) between two devices when a consumer uses their near-field communication (NFC) smartphone to pay, bill, buy tickets, utilize loyalty programs, prove their identity, or get access to restricted areas. An enemy who has an antenna may take advantage of this by intercepting or altering the sent signals. Many scholars have put up Near Field Communication (NFC) authentication systems to tackle this problem. However, the transactions still lack security and fairness. We provide an approach that ensures mutual authentication, security features, and excellent fairness. Mutual authentication is a security mechanism that prevents replay attacks and man-in-the-middle attacks. As far as trust between the parties concerned, equitable exchange, and transaction security are concerned, there are several issues with electronic transactions. Using a safe offline session key generation technique, the suggested protocol ensures more secure transactions and, most crucially, keeps our system lightweight while maintaining the fairness criterion. We found that when compared to competing protocols, ours offers superior performance in three key areas: transaction security, fairness, and low-weight protocol implementation. The proposed protocol's resilience and soundness are checked using Scyther, AVISPA (automated validation of internet security protocols and applications), and BAN logic. Formal proofs for security protocols are provided by AVISPA. As an added bonus, our protocol may mediate conflicts when one party behaves badly.

Abouhogail, Reham. (2019) Given the increasing number of mobile applications, ensuring their security has become more crucial. That is, especially when such applications include monetary exchanges. These days, one of these major topics is near-field communication (NFC) technology for mobile payments. In this paper, we introduce the NSLA protocol, a novel, lightweight, and secure authentication mechanism for NFC mobile payments. An innovative method for updating user identities and valid session keys is introduced by the NSLA protocol to ensure system security and secrecy. By looking at how well the NSLA protocol works, we can see that it uses very little processing power. Additional security testing has shown that the NSLA protocol is resistant to assaults such as denial of service, brute force, and replays.

Bojjagani, Sriramulu & Sastry, V (2019) Near Field Communication (NFC) is a promising technology that has recently gained traction due to the proliferation of mobile payments that rely on proximity. Here we provide a secure architecture for P2P and P2M payments that make use of near field communication (NFC). This method of payment uses elliptic curve cryptography (ECC) to safeguard private customer data. The suggested protocol allows the customer and retailer to communicate securely from beginning to finish by use of a bank-based reader and writer app. The acquiring bank validates and double-checks the amount on the merchant's device after users enter the customer PIN and the amount on their own NFC devices. We propose this strategy primarily to achieve this end. Customers may simply use their near-field communication (NFC) phones to enter their data, which may then be tapped into the retailer's NFC device, according to the proposed concept. Simulations employing automated validation of Internet security protocols (AVISPA), Scyther, and Tamarin, in addition to formal techniques of theoretical proof using Burrows-Abadi-Needham (BAN) logic, validate the correctness and security aspects of the presented strategy. The proposed system provides reduced transmission costs, lower processing overhead, and more security features than existing NFC payment methods in use today.

Badra, Mohamad & Borghol, Rouba (2016) Presented here is an encrypted method of mobile payment processing that makes use of the Near-Field Communication (NFC) radio interface. The proposed method uses symmetric cryptographic primitives; it is very lightweight; and it works on devices with limited memory and CPU resources. We demonstrate that our technique is cost-effective, simple to scale, and has little computational processing overheads while keeping NFC communications secure.

Ahamad, Shakeel et al., (2016) We provide a biometrically-based secure near field communication (NFC) mobile payment protocol that makes use of wireless public key infrastructure (WPKI) and universal integrated circuit cards (UICC). The protocol creates certified electronic signatures because it employs UICC, a device that is difficult to tamper with. To ensure that the issuer's or bank's mobile payment app stands out on the UICC, they might follow this procedure. Our SNMPB effectively handles stakeholder disputes by making use of capabilities like cryptographic audit logs, forensics mode, transaction counters, and transaction logs. By enforcing security measures at each step, from the UICC mobile payment app to the bank server, SNMPB ensures privacy, authenticity, integrity, and non-repudiation, and does away with the risk of overspending or repeat payments. We discovered that SNMPB is impervious to replay, man-in-the-middle (MITM), impersonation, and multi-protocol attacks after thoroughly validating it using BAN logic and the Scyther tool.

Pourghomi, Pardis et al., (2013) Smartphones, tablets, personal digital assistants, computers, and other mobile devices may now send and receive data without touching each other thanks to Near Field Communication (NFC), a kind of short-range radio communication. Near field communication (NFC) technology allows for contactless payment, which is one of its key properties. Customers may pay for goods and services using their NFC-enabled smartphones. Plus, customers have the option to use applications that utilize near-field communication (NFC), such as loyalty programs and tickets. Fears regarding the safety and efficiency of NFC deployment and use have kept the public from fully embracing and using the technology. Finding out how people like and react to this new form of payment and what happens when different countries try out near-field communication (NFC) systems is the main reason for these experiments. Due to the absence of a complete set of standards for managing the relationships between ecosystem stakeholders and the ownership of different NFC applications that contain sensitive information, issues with personalization, flexibility, manageability, and card personalization have emerged in the NFC ecosystem. Our study examines several Secure Element (SE) architectures and argues that cloud computing's ability to facilitate mobile payments could solve some of the issues now plaguing near field communication (NFC) payments.

III. EXPERIMENTAL SETUP

While conducting NFC-SET transactions, we want to verify the specified security services, which include confidentiality, authentication, no-replay, integrity, and non-repudiation. Therefore, due to its power and open source nature, we have selected the model checker by AVISPA tool.

A. AVISPA

The acronym for "Automated Validation of Internet Security Protocols and Applications" is AVISPA. Multiple back-ends using a range of cutting-edge automated analysis methods are part of the AVISPA project, which provides a modular and semantic formal language for analyzing protocols and their security aspects. As for the backend, they are:

- On-the-fly Model-Checker (OFMC)
- SAT-based Model-Checker (SATMC)
- Constraint-Logic-based Attack Searcher (CL-AtSe)
- TREE AUTOMATAS based on Approximations for Security Protocol Analysis (TA4SP)

B. Validation

We use High-Level Protocol Specification Language (HLPSL) code to create our 8 scenarios, which can be processed by AVISPA, to establish that our security approach is efficient. Therefore, an HLPSL Agent code describing the behaviors while sending or receiving messages is encoded into each entity (Card_EmulationHolder, Merchant, and Payment_Gateway). Afterwards, we construct sessions by merging two or three entities, based on the situation we are verifying. An instance of a session with three agents is "Session(C_em, M, P)" in scenario 1. An intruder or hacker may assume the identity of any agent by substituting the variable 'i' for the real agent. That way, he may read all of the messages transmitted to the compromised agent. Hackers' expertise reveals a number of characteristics, including the nature of the communication and the level of security. The hacker is already aware with certain factors, such as channels, hash functions, participant IDs, etc. The intruder may attempt to breach the security outlined in the "Goals" section of the HLPSL environment code by combining this information with data intercepted or received via protocol checking. This would work, provided that the necessary keys are known. We define the environment, which includes sessions, information on intruders, and security objectives, after we define the sessions. After responsibilities have been established, we move on to the details.

- It is assumed that the intruder is aware of all the security settings, including the hash function, the public keys of the participants, and their identities. The concept of "intruder-knowledge" provides this information.
- Given by "composition" is the number of sessions.
- The "Secrecy of" in the GOAL section grants the "Referred Service" of privacy. All encrypted and transferred data, including session keys, payment info, control data, card dealer number, and bridge answer, will be double-checked for confidentiality.

Scenario 1: All encrypted communications are verified during session establishment, confirming that the protocol is secure and ensures privacy in single-session (mono-session) execution.

Scenario 2: When multiple sessions are initiated, the number of visited nodes increases significantly. Due to exponential growth in response time, AVISPA effectively supports up to three sessions for multi-session security analysis.

Scenario 3: An intruder successfully initiates a session with the client by impersonating the merchant using the intruder's public key instead of the legitimate merchant's key.

Scenario 4: The attacker initiates a session with the merchant by impersonating the client. Despite this attempt, AVISPA confirms that the protocol remains secure.

Scenario 5: Mutual agreement on the shared key value between buyer and seller is ensured. Authentication and no-replay mechanisms confirm that the shared key is freshly generated and not reused from previous sessions.

Scenario 6: The protocol maintains security when the fifth scenario is extended to real multi-session execution.

Scenario 7: An intruder session is introduced as a valid client in the multi-session environment, and the protocol continues to operate securely.

Scenario 8: An intruder session impersonating a legitimate merchant is added, and the protocol remains secure under this attack model.

IV. RESULTS AND DISCUSSION

The following tables summarize all of the outcomes. Tables I, II, and III show the results of the validation for our eight scenarios with the ATSE, OFCM, and SATMC back ends, respectively. They confirm and respect the previously stated security objectives in every circumstance.

Table 1: OFMC Backend Evaluation Results for NFC-SET Protocol Security

Mode	Scenario	Attack Found	Upper Bound Reached	Encoding Time (s)	if2sate Compilation Time (s)
Authentication + Not Replay	mono-session	false	True	0.02	1.36
	multi-session	false	True	0.03	1.41
	hack-client	false	True	0.03	1.48

	hack-merchant	false	True	0.02	1.45
Confidentiality	mono-session	false	True	0.02	1.39
	multi-session	false	True	0.03	1.44
	hack-client	false	True	0.02	0.92
	hack-merchant	false	True	0.03	1.52

The new results from the AVISPA formal verification utilizing the OFMC backend confirm that the NFC-SET protocol is still safe in all the cases that were looked at. The absence of attacks seen in both confidentiality and authentication with non-replay modes across mono-session, multi-session, hack-client, and hack-merchant settings showed that the system was quite resistant to normal adversarial behaviors. The constant "false" result in the Attack Found column shows that the protocol fulfills the given security standards.

The OFMC model checker had strict search limits, and the protocol execution was extensively examined within those limits. In all cases, the upper bound was reached. This makes sure that the verification procedure doesn't terminate too soon and that the results are correct. The state-space complexity changed a little from one case to the next, notably in multi-session and hack-based models. This is why the encoding and if2sate compilation durations were somewhat different. The hack-client scenario operating in secrecy mode has reduced compilation times, which suggests that there is less symbolic complexity when there are no strict authentication requirements.

Table 2: ATSE Backend Evaluation Results for NFC-SET Protocol Security

Property	Scenario	Time (s)	Visited Nodes	Plies
Authentication + Not Replay	mono-session	0.09	8	5
	multi-session	10.82	1386	11
	hack-client + multi-session	0.31	37	8
	hack-merchant	4.26	924	6
Confidentiality	mono-session	0.11	8	5
	multi-session	16.47	1386	11
	hack-client	1.36	154	9
	hack-merchant	0.07	6	4

Recent results from the AVISPA validation tool using the ATSE backend show once again that the NFC-SET protocol is safe in a wide range of hostile and operational settings. The protocol's robustness against replay attacks and unauthorized information disclosure was proved when it successfully completed verification for both non-replay and secrecy parts of authentication.

Because single-instance executions had simpler protocols, the mono-session scenarios only looked at a small number of nodes and didn't require much time for verification. As expected given the larger state space created by running several protocols at the same time, the multi-session scenarios revealed a big rise in verification time, nodes visited, and plies. This shows that the ATSE backend can handle complex interaction patterns while still making sure that all data is thoroughly analyzed.

The protocol effectively constrains the capabilities of attackers, even under the assumption of partial system breach, as seen by the limited investigation depth and verification time observed in hack-based scenarios. The ATSE analyzer seems to be effectively eliminating dangerous paths, as seen by the comparatively short time and node count in hack-merchant situations when in secrecy mode.

Table 3: SATMC Backend Evaluation Results for NFC-SET Protocol Security

Property	Scenario	Analysed States	Reachable	Translation Time (s)	Computation Time (s)
Authentication + Not Replay	mono-session	4	3	0.03	0.01
	multi-session	240	231	0.07	5.62
	hack-merchant	7	4	0.03	0.02
Confidentiality	mono-session	6	4	0.03	0.03
	multi-session	240	231	0.07	5.81
	hack-client (mono-session)	240	231	0.06	0.71
	hack-merchant	0	0	0.01	0.00

The updated SATMC backend results of the AVISPA validation tool show that the NFC-SET protocol fulfills both the authentication with non-replay and secrecy criteria in all evaluated cases. Because there are just a few states that may be reached and examined in single-session runs, it is feasible to check quickly with practically no translation or computation time. This shows that the protocol is compact and well-structured.

In contrast, the number of states that could be analyzed and accessed increased significantly in multi-session scenarios, indicative of the bigger state space generated by concurrent protocol instances. It is well known that finding a solution to a constraint is hard in SAT-based model testing, therefore it is not unexpected that this spike resulted to longer computation times. The protocol's strength when run at the same time was shown when the SATMC backend passed verification without finding any security holes. The protocol tends to prevent harmful impacts even when partial penetration is assumed, as evidenced in hack-based scenarios like hack-client and hack-merchant models, which show limited state exploration and very short calculation time. In secrecy mode, the hack-merchant scenario didn't leave any usable attack traces since there are no states that can be accessed.

V. CONCLUSION

To sum up, NFC-SET will be a strong and reliable base for making contactless payment systems safer. NFC-SET combines the well-known security concepts of the Secure Electronic Transaction protocol with the ease and speed of NFC technology to solve major security problems with wireless transactions. The protocol will protect private data, stop replay and impersonation attacks, and make sure that all transactions are valid. It will also provide a secure system for online payments. NFC-SET would considerably reduce the hazards that come with short-range wireless communication by leveraging cryptographic techniques including encryption, digital signatures, and secure key management. Formal verification results will show that the protocol is safe in single-session, multi-session, and attacker-oriented contexts. This validation will prove that the protocol can work reliably in difficult operating situations by showing that it can handle both aggressive and passive assaults. NFC-SET will assist protect the growth of mobile commerce by offering modern digital ecosystems a transaction system that works well and can grow. A lot of people will utilize it, which will help NFC-based payment systems, boost consumer trust, and make financial transactions safer. So, near field communication security technology (NFC-SET) will be a good way to keep contactless payment systems safe in the future.

REFERENCES

[1] S. Ahamad, I. Alshourbaji, and S. Al-Janabi, “A secure NFC mobile payment protocol based on biometrics with formal verification,” *Int. J. Internet Technol. Secure Trans.*, vol. 6, no. 2, pp. 103–128, 2016.

[2] M. Badra and R. Borghol, “A lightweight security protocol for NFC-based mobile payments,” *Procedia Comput. Sci.*, vol. 83, no. 2, pp. 705–711, 2016.

[3] S. Bojjagani and V. Sastry, “A secure end-to-end proximity NFC-based mobile payment protocol,” *Comput. Stand. Interfaces*, vol. 66, no. 1, pp. 1–21, 2019.

[4] R. Abouhogail, “A new secure lightweight authentication protocol for NFC mobile payment,” *Int. J. Commun. Netw. Inf. Secur.*, vol. 11, no. 2, pp. 283–289, 2019.

[5] C. Thammarat, “Efficient and secure NFC authentication for mobile payment ensuring fair exchange protocol,” *Symmetry*, vol. 12, no. 10, pp. 2–19, 2020.

[6] S. Ahamad, “A novel NFC based secure protocol for merchant transactions,” *IEEE Access*, vol. 10, no. 2, pp. 1–11, 2021.

[7] P. Pourghomi and G. Ghinea, “Cloud-based NFC mobile payments,” *J. Internet Technol. Secure Trans.*, vol. 2, no. 4, pp. 1–19, 2013.

[8] D.-T. Kao, “The impact of transaction trust on consumers’ intentions to adopt m-commerce: A cross-cultural investigation,” Cyberpsychol. Behav., vol. 12, no. 2, pp. 225–229, 2009.

[9] J.-H. Yang and C.-C. Chang, “An efficient three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments,” J. Syst. Softw., vol. 82, no. 9, pp. 1497–1502, Sep. 2009.

[10] P. F. Schilke, O. Schierz, and B. W. Wirtz, “Understanding consumer acceptance of mobile payment services: An empirical analysis,” Electron. Commer. Res. Appl., vol. 9, no. 3, pp. 209–216, 2010.

[11] S. Weir, G. Douglas, T. Richardson, and M. Jack, “Usable security: User preferences for authentication methods in e-banking and the effects of experience,” Interact. Comput., vol. 22, no. 3, pp. 153–164, 2010.

[12] L. Kanniainen, “Alternatives for banks to offer secure mobile payments,” Int. J. Bank Mark., vol. 28, no. 5, pp. 433–444, 2010.

[13] T. Zhou, “The effect of initial trust on user adoption of mobile payment,” Inf. Dev., vol. 27, no. 4, pp. 290–300, 2011

[14] J.-S. Wang, F.-Y. Yang, and I. Paik, “A novel e-cash payment protocol using trapdoor hash function on smart mobile devices,” Int. J. Comput. Sci. Netw. Secur. (IJCSNS), vol. 11, no. 6, pp. 12–19, 2011.

[15] J. T. Isaac and S. Zeadally, “An anonymous secure payment protocol in a payment gateway centric model,” Proc. Comput. Sci., vol. 10, no. 4, pp. 758–765, Jan. 2012.

[16] E. L. Slade, M. D. Williams, and Y. K. Dwivedi, “Mobile payment adoption: Classification and review of the extant literature,” Mark. Rev., vol. 13, no. 2, pp. 167–190, 2013.

[17] T.-K. Chang, “A secure operational model for mobile payments,” Sci. World J., vol. 2014, no. 3, pp. 1–14, Oct. 2014.

[18] S. L. Javan and A. G. Bafghi, “An anonymous mobile payment protocol based on SWPP,” Electron. Commer. Res., vol. 14, no. 4, pp. 635–660, Dec. 2014.

[19] P. Van der Boor, P. Oliveira, and F. Veloso, “Users as innovators in developing countries: The global sources of innovation and diffusion in mobile banking services,” Res. Policy, vol. 43, no. 9, pp. 1594–1607, 2014.

[20] F. Liébana-Cabanillas, J. Sánchez-Fernández, and F. Muñoz-Leiva, “Antecedents of the adoption of the new mobile payment systems: The moderating effect of age,” Comput. Hum. Behav., vol. 35, no. 1, pp. 464–478, 2014.

[21] V. Odelu, A. K. Das, and A. Goswami, “SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms,” *IEEE Trans. Consum. Electron.*, vol. 62, no. 1, pp. 30–38, 2016.

[22] G. Nejad, T. Apanasevic, J. Markendahl, and N. Arvidsson, “Stakeholders’ expectations of mobile payment in retail: Lessons from Sweden,” *Int. J. Bank Mark.*, vol. 2, no. 4, pp. 12–21, 2016.

[23] A. Chaudhry, M. S. Farash, H. Naqvi, and M. Sher, “A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography,” *Electron. Commer. Res.*, vol. 16, no. 1, pp. 113–139, 2016.

[24] R. Sureshkumar, R. Anitha, N. Rajamanickam, and R. Amin, “A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity,” *Comput. Electr. Eng.*, vol. 57, no. 2, pp. 223–240, 2017.

[25] Masihuddin, B. U. I. Khan, M. Mattoo, and R. F. Olanrewaju, “A survey on e-payment systems: Elements, adoption, architecture, challenges and security concepts,” *Indian J. Sci. Technol.*, vol. 10, no. 20, pp. 1–19, 2017.

[26] F. Liébana-Cabanillas, I. Ramos de Luna, and F. Montoro-Ríos, “Intention to use new mobile payment systems: A comparative analysis of SMS and NFC payments,” *Econ. Res.-Ekon. Istraž.*, vol. 30, no. 1, pp. 892–910, 2017.

[27] R. Bojjagani and V. Sastry, “A secure end-to-end SMS-based mobile banking protocol,” *Int. J. Commun. Syst.*, vol. 30, no. 15, pp. 2-5, 2017.

[28] A. Yohan, N. W. Lo, and D. Winata, “An indoor positioning-based mobile payment system using Bluetooth low energy technology,” *Sensors*, vol. 18, no. 4, pp. 1-8, 2018.

[29] J. Xu, K. Xue, Q. Yang, and P. Hong, “PSAP: Pseudonym-based secure authentication protocol for NFC applications,” *IEEE Trans. Consum. Electron.*, vol. 64, no. 1, pp. 83–91, 2018.

[30] S. Thammarat and W. Kurutach, “A secure fair exchange for SMS-based mobile payment protocols based on symmetric encryption algorithms with formal verification,” *Wireless Commun. Mobile Comput.*, vol. 2018, no. 6, pp. 1–21, Jul. 2018.