PERA-Pay: A Power-Efficient and Robust Architecture for NFC Payment Systems

Ali Ghasemi
Amirkabir University of Technology
Tehran, Iran
s.ali.ghasemi001@aut.ac.ir

Carol Fung
Concordia University
Montreal, Canada
carol.fung@concordia.ca

***Abstract*—Near Field Communication (NFC) is a widely utilized wireless communication technology, particularly in smart cities and payment systems. However, its safety remains a significant concern due to vulnerabilities to threats such as relay, replay, and man-in-the-middle. An advanced relay model using wearable passive relays recently extended the NFC communication range to over 49.6 centimeters, which raised huge concerns among users. Despite prior efforts to enhance protection, new relay threats persisted at the architectural level. To address these concerns, we proposed PERA-Pay, an enhanced architecture for payment systems that are compliant with the NFC-based contactless specification and designed to resist relay invasions in both traditional and mobile payment systems. Our approach strengthens the payment system through a prediction model and a challenge-response scheme with extended key generation through an energy-efficient architecture. This architecture also effectively protects not only against traditional hardware-level invasions but also against advanced relay threats. The evaluation demonstrated that PERA-Pay improves NFC payment safety by preventing modern relay threats, while reducing energy consumption significantly against the base system and the state-of-the-art as well, an aspect overlooked in prior research.**

***Index Terms*—Near-field communication, Contactless payment system, Emerging architectures, Energy efficiency, IoT.**

I. Introduction

The Internet of Things (IoT) has transformed various domains, such as smart homes and industrial systems, by enabling seamless connectivity and data-driven operations. However, this widespread integration also raises significant concerns where sensitive personal information, including payment data, may be exposed to unauthorized individuals [1]. Therefore, ensuring the security and privacy of IoT systems is critical, requiring robust encryption and adherence to stringent data protection standards [2]. Near Field Communication (NFC) payment is a contactless method that enables users to complete easy payments by bringing their NFC-enabled devices near an NFC reader [1]. Security in NFC payment systems is critical because it involves money transfers and financial data. [3]. In a relay attack, the attacker uses proxy devices to forward data between a victim's smart card and a reader, enabling unauthorized payments. In another instance, the attacker can save, modify, and later use the information through the intermediary parties, which is called a man-in-the-middle attack.

Many attacks to NFC can be mitigated by deploying advanced encryption techniques, multi-factor authentication, anomaly detection, and enhancing the protocol layer security [4], [5]. Yet, advancements in manufacturing technology and hardware complexity have shifted attackers' focus toward exploiting vulnerabilities at the hardware level. Notably, recent successful hardware-level attacks (e.g., ReCoil attack [6]) bypassed common security measures, emphasizing the need for enhanced hardware design methods. Although many techniques have been proposed [5], [7]–[9], they are unable to protect against the new hardware-level attacks, and they have some shortcomings, such as high delay and energy consumption overhead. The new attack model harvests more energy from the NFC reader to expand the communication range and decrease the transaction delay through strengthened attack devices. Since the advanced model of the ReCoil attack can finish transactions in less than the defined threshold time of common relay-attack detection methods, the existing delay-based approaches can not detect it, and so NFC payment systems continue to be vulnerable. This is the first study to handle the advanced attack model. Besides, prohibiting other attacks also requires much time and energy to process cryptography keys beyond conventional methods [8].

In this study, we propose an enhanced NFC payment design called PERA-Pay that resists new hardware-level attacks with low delay challenge response and communication cost. In addition, it can protect against advanced ReCoil attack efficiently by providing strategies such as power-efficient in-situ computing of exchange keys to find real responses and detect high-power usage of attackers from the reader device. The innovative deep learning model is also adopted to predict unauthorized interactions in the preprocessing phase. Our system enhances the security of payment systems, which is tested by Scyther [10]. We implemented and evaluated the architecture's power consumption and safety by Arduino-based setup, Gem5 [11]-based cycle-accurate simulator and NVSim [12]. The evaluation results show that PERA-Pay reduces the power consumption by 1.56x and 2.89x (w/ HW level design) on average in comparison to previous studies. Additionally, our system demonstrates an accuracy of 93% in detecting unauthorized transactions with the assistance of the prediction model.

The contributions of this paper can be summarized as follows. 1) We designed a novel energy-efficient NFC-based architecture to resist new hardware-level attacks, including

978-3-903176-75-1 ©2025 IFIP

ReCoil attack, based on the power usage of devices and challenge-response between parties. 2) We proposed an in-situ computing component to generate secret or shared keys, and designed efficient message model and execution flow to protect NFC interactions with low power consumption and communication overhead. 3) We adopted a deep learning-based preprocessing phase to raise the accuracy level and enhancement in in-situ operations of our system by unauthorized relayed signal classifying transactions.

II. Literature Review

NFC payment systems offer flexibility but face security and efficiency challenges, including critical attacks and high energy consumption [13]. Numerous types of attacks, including relay attacks [6], and replay attacks, can threaten payment systems. Practically, [6] presents a new experimental assessment conducted on commercial NFC that reveals the ability to relay signals over an extended range of 49.6 centimeters. A new architecture-based attack model harvests high energy from the reader device, facilitating relay attacks beyond regular models and jeopardizing the common protection methods.

Various countermeasures [4], [5], [14], [15] can be divided into the following groups, which are more related to our scope. The paper [4] proposes NFC relay detection methods using signal fingerprinting, achieved by designing deep learning and evaluating on NFC relay attacks. Other solutions, such as cryptographic enhancements by efficient hashing (e.g., the Chaskey algorithm [8]), aim to strengthen authentication. As an example of protocol-based approaches, the Distance Bounding Algorithm [14] measures the round time trip for security. Furthermore, the N-Guard Protection study focuses on improving the security of NFC-based systems. It enhances NFC security on smartphones with firmware changes, blocking unauthorized transactions using a high level approach [7]. The paper [5], proposes a protocol enhancing an NFC-based mobile payment with a secure anonymous authentication mechanism and unique session keys. Additionally, [9], [15] are contactless payment systems that aim to establish defenses against relay attacks. They suggested relay-protection protocol-based and abstract-level approaches. The latter also utilizes a cloud-based system to manage and process time and data securely. This technique has notable shortcomings, including security issues and simple relay attacks, which remain a concern as the system struggles to detect and inhibit new attack model.

While the studies provide valuable insights, they fall short in addressing new architecture-level threats. Current countermeasures can not detect advanced relay attacks that mimic normal signals within RTT with expanded range and low delay. Also, they lack protection against all kinds of attacks efficiently, while also introducing power and communication overhead. Hence, we need to suggest an enhanced security architecture to prevent new architecture and ReCoil attacks by providing a new challenge response element in our design to find the relayed signals and a secret key method to compute in place with real-time generated parameters. Moreover, we can mitigate the communication overhead and energy consumption

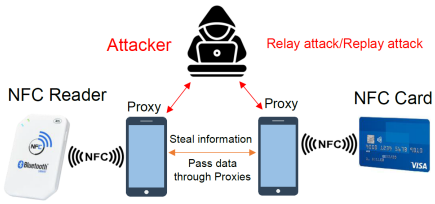

Fig. 1. Introduction to the NFC payment system and its security shortage

of the system by locating and diminishing the extra power usage of the reader device.

III. PERA-Pay method

In this section, we present PERA-Pay, a smart and efficient NFC-based contactless system to combat new attack models further than the previous studies. We first present critical attack models, followed by an overview of our preprocessing phase, and an energy-efficient architecture with a novel in-situ key encryption and data organizer.

A. Relay and hardware level attacks

A relay attack occurs when an attacker intercepts and forwards communication between two parties without permission, potentially modifying the content. For example, as shown in Fig.1, an attacker exploits the weak systems to perform a replay or relay attack by proxy devices. The data can be modified or directly transferred leading to accomplishing payment transactions without distraction and detection. Indeed, the proxies helped to relay signals between the NFC card and the reader to expose themselves as real devices and simulate that they are close to each other. Although many solutions [5], [7]–[9] have been proposed to address the security problems in NFC payment systems, they overlook architecture layer attacks and often incur high costs, latency, and energy consumption. The [6] developed a wearable device with multiple coils and variable capacitors to direct near-field signals, enhancing power delivery to NFC cards over greater distances. In the advanced attack model, passive relays are optimized to absorb maximum energy from the NFC reader, extending communication range by adjusting coil geometry for peak performance to conduct the relay attack.

B. Overview of PERA-Pay

To overcome the drawbacks of the countermeasure methods mentioned in the prior section, we propose PERA-Pay, an AI-driven defense system that can detect the new architecture-level attack and ReCoil with in-place challenge response. In our method, the first step is the preprocessing phase, including data wrangling and classifying it by deep learning and models to enhance our method's accuracy and predict the fake signals. Pre-processing phase also leads to diminished overhead in the PERA-Pay's architecture and maps data into it efficiently. Secondly, the major part of our method is HW/SW, which is a combination of architecture and protocol layers. It includes a novel in-situ efficient emerging NFC architecture to improve security and energy saving towards a secure session key generator, which includes extra parameters to find the real transaction period time. Our architecture design also detects

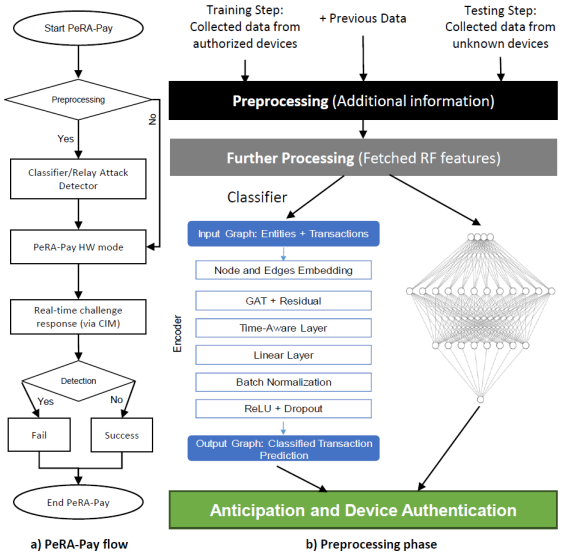

Fig. 2. Pre-processing phase, including anticipation and classifier model

the extra absorbed energy from the reader to discover and inhibit the probable attack through an in-situ computing model. These allow us to prevent various attacks, such as replay and new relay attacks, with low communication overhead.

C. Preprocessing phase (NFC attack prediction model)

This step is a pioneer and booster for the main architecture to detect and anticipate unauthorized signals and transactions in payment systems. As shown in Fig. 2, part 1 is (a) an abstract flow of our system, and given part (b) depicts the preprocessing phase in detail, which our design can work in two separate or combined modes. Using Convolutional neural network (CNN) and Graph Neural Networks (GNN) in our study, as previous studies depicted that CNNs are so appropriate in RF fingerprinting tasks on signals, and GNNs have proven highly effective for classifying the data, like ambient conditions, as well [4].

First, we proposed the CNN model to detect and anticipate probable relayed signals to prevent relayed attacks, raise the accuracy level, and reduce the overhead of the architecture. Waves are gathered to discover the differences between relayed and non-relayed waves for card-based transactions and collected under varying ambient conditions for mobile devices. The similarities in these conditions enable to identification of the relay attack if the signals of the conditions are not the same. A CNN is employed, utilizing 4 normal signals, 2 wireless relay attacks, and 2 wired relay attacks. As shown in Fig. 2, this CNN consists of 3 convolutional layers and 1 fully connected layer, incorporating 72 kernels of size 8, 64 kernels of size 6, 32 kernels of size 6, and 256 hidden units. Moreover, quantization in CNNs reduces computational complexity and memory usage by converting high-precision values (e.g., 32-bit floats) to lower-precision formats (e.g., 8-bit integers). The data pattern and parameter size of CNN-based models derived from [4] study. We compared separable and regular CNNs to detect RF fingerprint features in signals, identifying relayed waveforms from attackers.

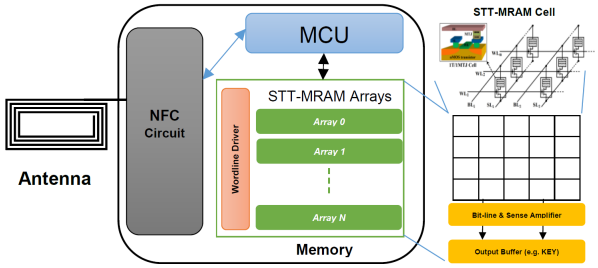

Fig. 3. The abstrace schematic of our novel design

Furthermore, we integrated GNN to classify transactions to prevent further attacks, even fraud payments. Detail of the GNN is illustrated in Fig. 2 as well. The process begins with the input graph, derived from our dataset features, and ends with the Output Graph, which utilizes a multi-layer perceptron to assess transaction legitimacy, classifying and setting a probability for the group. The final output is a graph where transactions are labeled as 1 or 0, facilitating effective detection in payment networks. The grouped data provides an efficient mapping to our architecture and embed in its limited resources, leading to even online detection in PERA-Pay by using in-situ computing components. To substantially reduce the peak memory cost of running models, we offer a quantization-aware training that diminishes model size, integrates complementary rescheduling strategies and mapping: in-place memory rescheduling within and maximizing the utilization of computing resources. It is customized to be used in PERA-Pay design and its emerging structure to augment the accuracy of entire process despite the reducing file size.

D. Energy-efficient design and execution flow

According to PERA-Pay architecture, the pre-processing phase helps to discover possible attacks by utilizing the graph classifier. In fact, grouped data, which is divided into small parts, can be mapped in the in-situ design of the architecture efficiently to process the online data in a critical situation. Furthermore, we designed a novel architecture that enables us to compute the customized shared keys quickly and power efficiently. Our design is depicted in Fig. 3, containing a microcontroller unit (MCU) and an innovative memory array design (STT-MRAM based) which roles as both a data storage and a session key processor. STT-based memory comprised flexible arrays in addition to the bit-line, sense amplifier to accumulate and digitize the data, which are followed by a customized output buffer putting out the final value. It also has other elements such as an antenna and an NFC circuit as an NFC tag/reader device. The solution has included a new key generation model in both the reader and the NFC smart card through in-situ computing for each verification process. It addresses the advanced relay attack and ReCoil by locating real interactions if parties respond to the challenges in the identified time window correctly.

More specifically, we proposed an approach including a new challenge-response time approach in place (time) to ensure the signals are secure and get the responses within the defined time (ns). Defined time is equivalent to time +

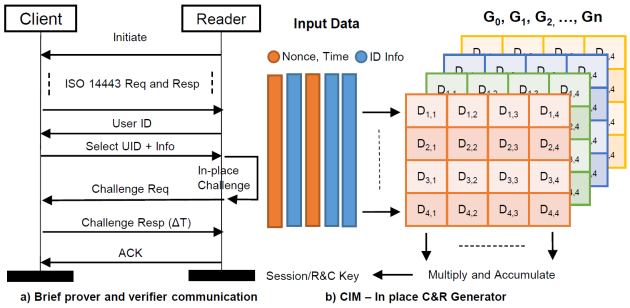

Fig. 4. Strategy of Input and weight encryption in the PERA-Pay architecture

nonce + one identity information. In-situ computing, especially in response-challenge, causes the communication overhead to be diminished, and the system can protect against all relay attacks by generating a random secret time between parties in place, detecting fake signals. For instance, a hashed-in-time/response-challenge message is generated by parameters like (ID, GENERATED_VALUE, and TIME/Energy(NFC Reader)). It generates a trustworthy key and noniterative threshold value for each transaction, allowing us to have a safe transaction regardless of the distance between the prover and verifier. If both parties respond to the challenge in a similar manner within the specified time, the transaction will be secure and proceed to completion. Therefore, the PERA-Pay prevents advanced architecture-level attacks with additional useful attributes by negligible overhead.

According to the low-level design of our payment system, we can detect high absorbing (ReCoil and advanced attack model) and usage energy from the reader device by checking the energy consumption of the NFC devices in each transaction, either as integrated parameters for challenge response or distinguished. Moreover, our innovative memory design of the MCU is not only used to store secret parameters but also to compute shared keys efficiently. For instance, we can handle encryption and generating challenge/response issues directly within the memory by utilizing the STT-MRAM processing capabilities (in-place challenge) of the PERA-Pay model, as shown briefly in Figure 4 (a), which depicts the communication and messages between parties. Specifically, in Figure 4 (b), the data is arranged in a 4 × 4 matrix (Groups) and treated as a memory array for an n-bit key length. The input data, such as Identification, Time/Location, Energy, and a generated Nonce, undergoes five consecutive clock cycles, after which it is processed within the memory arrays and groups. In the final step, the keys are calculated using a Multiply Accumulate element. In addition, especially for this purpose, we explored and designed optimal strategies and STT-RAM memory parameters, which we have chosen and listed in Table I. As a result, by effectively managing and optimizing limited resources like the NFC tag/reader, we can enhance reliability and reduce energy consumption.

A suitable execution flow has also been suggested for PERA-Pay as seen in Fig. 5. The mentioned flow incorporates a secure database (DB) to manage data effectively. It enables the retrieval of essential data, such as customer identification

TABLE I
DESIGN PARAMETERS

Parameters	Value
Number of Arrays	2
Memory Size per Array	128×128 (4 KB each)
Word Width	8-bit (adjustable to 1-bit)
Computation Capability	Bitwise, small MAC operations, Matrix Multiplication
Energy Consumption	~30-50 µW
Physical Area	~0.4 mm²

The proposed flow (Transaction phase)

Local DB → Fetched internal memory → Customer ID, password
Access (Card Info) → Encrypted info = I_x
Computes I_x = ID || Password || Random number + Additional elements (e.g. Time)
The Receiver and Prover → connected to each other
Generated I_y = I_x + Receiver status
Check ID and I_x → Key and stored (NFC Tag)
If (Verified) → Convert Data → Payment Done
Else
If (Threshold > limitation is assigned by Additional Arguments) → Decline
OR
Not the same → Decline

Fig. 5. The suggested execution flow

information, directly from internal memory. Each access card contains an encrypted internal ID that reflects the memory status of the card, ensuring secure communication during transactions. The system's receiver and reader are interconnected to verify multiple operational parameters, which are dynamically generated based on the current status of the receiver. To ensure robust authentication, the system checks the validity of the internal ID against the key and stored status in the database. A set of thresholds, which is included and generated randomly in the challenge response as well, is established to enhance security, such as time and UID, causing differential model detection between parties to protect against relay attacks. If any parameter exceeds the high threshold or does not align with another part, the transaction is declined. Conversely, if the authentication process is successful, the data is converted into the appropriate format, allowing the payment to be processed seamlessly. The flow is integrated to the in-situ component and our embedded architecture to mitigate the challenge-response times and communication cost.

IV. EXPERIMENT AND RESULT

This section outlines the results of the experiments conducted to demonstrate the feasibility of the proposed method.

We implemented and launched HW/SW systems and devices for NFC communication, readers and tags, and our novel architecture that could help me evaluate the PERA-Pay as depicted in Fig. 6. It includes two Arduino Mega 2560 (microcontroller), PN532 (RFID module), one ESP32 as a small server, and one database, which is connected via NFC communication. As also seen in Fig. 6, we simulated the NFC smart card, reader, and server, which perform the

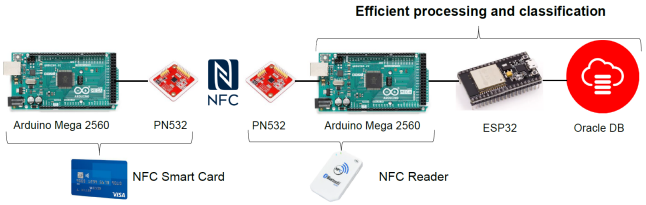

Fig. 6. The Arduino based system architecture for simulation

TABLE II
A COMPARISON OF THE ANTICIPATION MODEL ALONGSIDE PRIOR WORKS

System	File Size (kb)	Training Time (ms)	Testing Time (ms)	Accuracy
Secure NFC e-Payment	32976	2.399	1.201	81%
CARA method	71476	1.806	0.048	86%
N-Guard method	21864	1.198	0.618	91%
PERA-Pay method	10067	1.216	0.097	93%

core functions of the NFC-based payment system in this setup. It is noteworthy that we have customized the cycle-accurate simulator for implementing the emerging part of the PeRA-Pay architecture and calculating systems' power consumption. Many tools, such as Scyther [10], NVSim [12], and Gem5 [11], are used as well for designing our architecture and evaluating the security attributes and energy efficiency of the architecture. The security protocols of PERA-Pay have been analyzed using the Security Protocol Description Language (SPDL) in Scyther to evaluate encrypted communications. We also assume Android devices and new architecture relay attacks are attackers in the system. Besides, the experimental setup leverages the CardEmulator and TerminalEmulator Android applications, which function as NFC proxies to simulate real-world interactions.

A. The Data Pre-processing and Accuracy

To analyze pre-processing PERA-Pay, we evaluated our method and compared it with related works. The data sets used (66k samples, comprising 8 tag types, 4 normal and 4 wireless-relayed signals) consist of both randomly generated signals and those created following the approach in [4], saved as wave files. Specifically, we gathered data from about 1k transactions using sensors (e.g., WiFi, Location, Bluetooth) and ambient conditions for a mobile payment, while also simulating and collecting emitted waves from card-based systems in each transaction. A total of 1,000 signals were utilized, divided into two groups: 700 for training sets and 300 for testing data, containing faulty matrices to prove the reliability of the method. As shown in Table II, the preprocessing outperforms in comparison with previous studies and could get better results in accuracy and file size, which are crucial in payment systems to commit transactions with minimum error. However, it shows a little overhead in training time against the N-Guard method, which is negligible.

B. Safety and Energy consumption

We applied the proposed model using the Scyther tool to validate numerous authentication claims, as shown in Table III. The confidentiality claims such as Alive, Weakagree, Niagree, and Nisynch are employed to identify potential threats such as replay, relay, and man-in-the-middle attacks. As depicted in Table III, we have experimented with all the reachable paths

TABLE III
OUTCOMES OF RUNNING PERA-PAY ON SCYTHER TOOL

	Claim		Status		Comments
NFCLongT	**A**	Alive	**OK**	**Verified**	No attacks
		Weakagree	**OK**	**Verified**	No attacks
		Niagree	**OK**	**Verified**	No attacks
		NiSynch	**OK**	**Verified**	No attacks
		MS Secret	**OK**	**Verified**	No attacks
		Commit parties	**OK**	**Verified**	No attacks
	B	Alive	**OK**	**Verified**	No attacks
		Weakagree	**OK**	**Verified**	No attacks
		Niagree	**OK**	**Verified**	No attacks
		NiSynch	**OK**	**Verified**	No attacks
		MS Secret	**OK**	**Verified**	No attacks
		Commit parties	**OK**	**Verified**	No attacks
	C	MS Secret	**OK**	**Verified**	No attacks
		Niagree	**OK**	**Verified**	No attacks
		NiSynch	**OK**	**Verified**	No attacks
		Secret PI	**OK**	**Verified**	No attacks
		Secret Kx	**OK**	**Verified**	No attacks
	POS	Alive	**OK**	**Verified**	No attacks
		Weakagree	**OK**	**Verified**	No attacks
		Niagree	**OK**	**Verified**	No attacks
		NiSynch	**OK**	**Verified**	No attacks
		MS Secret	**OK**	**Verified**	No attacks
		Commit parties	**OK**	**Verified**	No attacks
	TP	MS Secret	**OK**	**Verified**	No attacks
		Niagree	**OK**	**Verified**	No attacks
		NiSynch	**OK**	**Verified**	No attacks
		Secret PI	**OK**	**Verified**	No attacks
		Secret Kx	**OK**	**Verified**	No attacks

TABLE IV
SPECIFIC RELAY ATTACKS COMPARISON

Method	Relay	ReCoil	Advanced HW-level attack
Baseline/Countermeasures	Yes	No	No
PERA-Pay (only challenge-response)	Yes	Yes	No
PERA-Pay (+HW)	Yes	Yes	Yes

from various perspectives, such as prover, verifier, novel verifier, and third parties named A, B, C, and TP, in our method, allowing us to prevent novel attacks as well. The outcomes illustrate the validity of all Scyther claims associated with our modified method, in addition to custom rules like mutual secrecy secret, relay attack, and identification secret, with no detected vulnerabilities. As a result, all possible scenarios are considered and "Verified" successfully. ReCoil and advanced hardware-level attacks are evaluated at the architecture level as well; the latter one attacks in low delay and with high energy harvesting, which are depicted in Table IV.

We also compared PERA-Pay with countermeasures, taking into account their energy consumption. The datasets have been collected in two different ways to guarantee the outcomes.

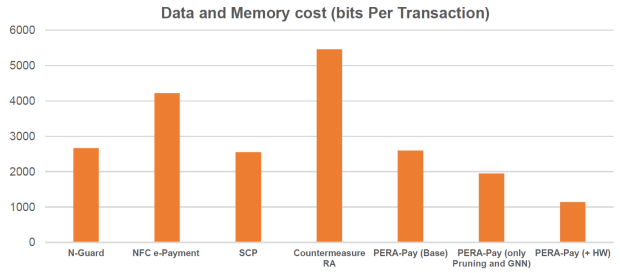

Fig. 7. Data and storage cost of the proposed methods

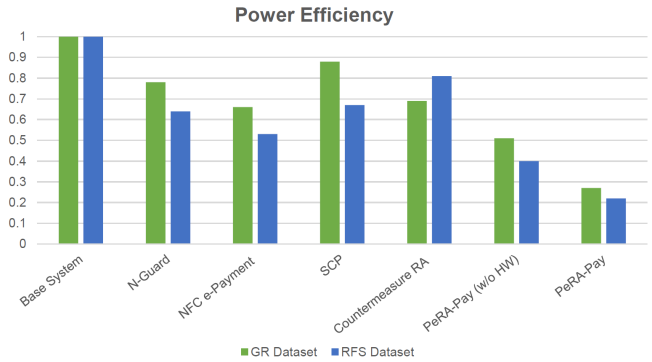

Fig. 8. Power consumption of various studies

The first one is a collected per-transaction dataset that is the same for all studies, and the second one is called RFS, which is imitated like an RF signal study [4]. In addition, a Gem5-based custom cycle-accurate architecture simulator is employed to evaluate the in situ processing, memory usage, and energy consumption of the PERA-Pay integrated with NVSim to simulate and evaluate in-situ STT-RAM design. The Fig. 7 shows the comparison of PERA-Pay and related works, indicating low memory cost of the method against previous studies, especially in the PERA-Pay model, in which we have taken into account all features of our architecture, including GNN and in-place processing. PERA-Pay can mitigate storage cost by removing extra messages between parties, such as receiving or saving random numbers, getting certification multiple times, and symmetric session keys in responses.

Moreover, our solution offers a notable reduction in power consumption consuming approximately 73% less energy on average compared to base system that shown in Fig. 8. We consider our proposed method in two schemas. The first one is just based on the high level approach without regard to novel and efficient architecture, and another one is corresponded to preprocessing plus architecture level. As Fig. 8 shows, results of the average of two datasets, illustrates the method and (method + our architecture as PERA-Pay) saves more energy against N-Guard Protection [7], Secure NFC e-Payment [8], Secure Contactless Payment (SCP) [5], and Countermeasure against relay attack [9] 1.56x, 1.30x, 1.71x, and 1.68x and (2.89x, 2.42x, 3.15x, and 3.11x) respectively.

In addition, our low-energy STT-MRAM-based design for generating keys leads to lower energy consumption. Prohibiting extra usage power beyond recent studies in NFC readers ultimately diminishes the power consumption. Thoroughly, that PERA-Pay has achieved energy improvement in energy consumption 1.56x and 2.89x on average in comparison to previous studies by influencing crucial attributes such as mitigating communication overhead through providing a novel in-situ computing component, which removes data transfer between processor and memory by computing in place.

V. Conclusion

NFC technology is widely used in payment systems, but faces security and energy issues. Considering those critical issues is crucial, especially in modern devices. Recent attacks, such as the ReCoil expanded range attack with low delay, expose serious risks. To address this, we developed a novel system that resists advanced attacks in NFC payments using improved energy-efficient architecture, in-situ computing of shared keys, and detection of classified signals. Evaluation showed it blocks modern attacks while cutting energy use by up to 2.89x compared to older systems. PERA-Pay can be a practical step forward for NFC technology, with the potential for broader applications. Despite the impressive improvement in security and energy consumption, there are still drawbacks to overcome in the future. For example, while our method extremely enhances both security and energy efficiency, it introduces a minor area overhead, which is negligible in comparison with the improvements. For future work, we will focus on area-efficient designs and application-layer enhancements for modern applications.

References

[1] P. Onumadu and H. Abroshan, "Near-field communication (nfc) cyber threats and mitigation solutions in payment transactions: A review," *Sensors*, vol. 24, no. 23, p. 7423, 2024.

[2] S. Szymoniak, J. Piatkowski, and M. Kurkowski, "Defense and security mechanisms in the internet of things: A review." *Applied Sciences (2076-3417)*, vol. 15, no. 2, 2025.

[3] S. Alshebli and C. Y. Yeun, "Examining the security landscape of mobile payment systems," in *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024, pp. 1–5.

[4] Y. Wang, J. Zou, and K. Zhang, "Deep-learning-aided rf fingerprinting for nfc relay attack detection," *Electronics*, vol. 12, no. 3, p. 559, 2023.

[5] A. M. Allam, "Privacy-preserving nfc-based authentication protocol for mobile payment system," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 17, no. 5, pp. 1471–1483, 2023.

[6] Y. Sun, S. Kumar, S. He, J. Chen, and Z. Shi, "You foot the bill! attacking nfc with passive relays," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1197–1210, 2020.

[7] R. Di Pietro, G. Oligeri, X. Salleras, and M. Signorini, "N-guard: a solution to secure access to nfc tags," in *2018 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2018, pp. 1–9.

[8] D. Clarisa and D. Marlena, "Design of secure nfc e-payment with ambient conditions-based solutions and chaskey algorithm," in *2021 6th International Workshop on Big Data and Information Security (IWBIS)*. IEEE, 2021, pp. 139–144.

[9] P. Li, H. Fang, X. Liu, and B. Yang, "A countermeasure against relay attack in nfc payment," in *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*, 2017, pp. 1–5.

[10] C. J. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols: Tool paper," in *International conference on computer aided verification*. Springer, 2008, pp. 414–418.

[11] J. Lowe-Power, A. M. Ahmad, A. Akram, M. Alian, R. Amslinger, M. Andreozzi, A. Armejach, N. Asmussen, B. Beckmann, S. Bharadwaj *et al.*, "The gem5 simulator: Version 20.0+," *arXiv preprint arXiv:2007.03152*, 2020.

[12] X. Dong, C. Xu, Y. Xie, and N. P. Jouppi, "Nvsim: A circuit-level performance, energy, and area model for emerging nonvolatile memory," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 31, no. 7, pp. 994–1007, 2012.

[13] A. Luntovskyy, T. Zobjack, B. Shubyn, and M. Klymash, "Energy efficiency and security for iot scenarios via wsn, rfid and nfc," in *2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*. IEEE, 2021, pp. 1–6.

[14] S. Mauw, Z. Smith, J. Toro-Pozo, and R. Trujillo-Rasua, "Distance-bounding protocols: Verification without time and location," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 549–566.

[15] A.-I. Radu, T. Chothia, C. J. Newton, I. Boureanu, and L. Chen, "Practical emv relay protection," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 1737–1756.