International Journal of Computational and Electronic Aspects in Engineering
Vol. 5, Issue 3, Sept 2024, pp 90-97
https://doi.org/10.26706/ijceae.5.3.20240803

An Encrypting Electronic Payments Based on Kerberos Cryptography Protocol

Hasan Abdal-Azal Abdulrazzaq Alsaiqal

Administrative and Financial Department, Ministry of Finance, Baghdad, Iraq

*Correspondence: Hasanalsaiqal77@gmail.com

Abstract: At present, the prevalence of mobile phones in the country and the availability of capabilities such as encryption, key generation, and authentication present an appropriate opportunity for a variety of payment platforms. The preparation of equipment and a comprehension of the technical possibilities and difficulties in this field are necessary to achieve this capability. This paper introduces a secure electronic payment system that utilizes the Kerberos cryptography protocol to guarantee authentication, integrity, and confidentiality. The system ensures secure transactions between users and merchants by utilizing the ticket-granting mechanisms of Kerberos and symmetric key encryption. It mitigates the risk of unauthorized access and fraud by guaranteeing that all parties are authenticated prior to the exchange of any payment information. This method addresses critical challenges in the digital financial environments of today by improving the trust and privacy of electronic payments. The proposed model effectively safeguards sensitive financial data while simultaneously ensuring user convenience. The experimental results demonstrate that the proposed method maintains robust security characteristics while simultaneously achieving high quality and low computing complexity.

Keywords: Mobile; Kerberos; Electronic Payments; Authentication; Cryptographic.

Article – Peer Reviewed
Received: 25 July 2024
Accepted: 17 Sept 2024
Published: 30 Sept 2024

Cite this article: Hasan Abdal-Azal Abdulrazzaq Alsaiqal, "An Encrypting Electronic Payments Based on Kerberos Cryptography Protocol", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 5, issue 3, pp. 90-97, 2024.
https://doi.org/10.26706/ijceae.5.3.20240803

1. Introduction

The intricate issue of electronic banking security arises from the prevalence of fraudsters who take advantage of any opening to mislead and pilfer money [1], [2]. A crucial component of banking operations, customer identification has evolved significantly over time. Because towns were tiny, bankers could rely on their firsthand knowledge of their customers' identities in an era before computers. Electronic banking, sometimes referred to as e-banking, evolved as automatic banking in a cashless world with the introduction of computers, the development of technology, and the proliferation of networks. Smart cards are becoming widely used, and this has improved security, but there are still certain weaknesses that need to be fixed, especially with e-banking. The use of e-banking via consumers' mobile phones has been made easier by wireless connection through mobile devices and smart cards, giving rise to what is today referred to as mobile banking, or m-banking. In order to strike a balance between user-friendliness and consumer safety, mobile banking keeps developing and provides increased security. Among the most important and widely used tools for transferring money internationally, mobile phones make it easier for people and businesses to deal with each other. Improving security measures is becoming more and more necessary as mobile devices are used in financial transactions. Even while encryption is essential for protecting the transit of information, it is not sufficient to meet all security requirements. Security protocols that improve the encryption process are thus also used [3], [25], and [26] .

Mobile banking payments have emerged as one of the most important and popular ways for people and businesses across the world to exchange value and move money. It is now more important than ever to improve information security and safeguard financial data across several communication networks as the use of these techniques has grown [4].

One of the most important tools for improving the security of financial data transfers is encryption. That being said, encryption is not enough to satisfy all security needs. The initial idea of the internet is very different from what it is today. Numerous dot-com businesses from the early days have either succeeded in earning money online or gone bankrupt. The problem of online payments is one of the primary obstacles still present. Three main causes are driving the growing need for new and enhanced payment methods for both online and offline purchasing. First, trading has become easier and more common than ever thanks to advancements in technology and information communication technologies. The spike in global logistics and support firms has resulted in the facilitation of product transportation across international boundaries; nevertheless, payment processing has encountered difficulties in these situations. Second, there are many new ways to cut expenses thanks to electronic payment systems. Third, the need for straightforward and safe online payment options has been fueled by the losses connected to the recent surge in online sales [5]–[7].

This study utilized the Kerberos protocol for safeguarding and decryption. Symmetric encryption was applied in addition to the key distribution center because the Kerberos protocol requires an external party to provide highly reliable authorization by establishing the identity of the user (SIM) for authentication. The trust manager's role is then to verify the identity of the other trusted party.

The remaining portions of the paper are structured as follows. Part 2 provides an explanation of the relevant work. Section 3 explains the idea of encryption in cryptography algorithms. Section 4 provides details on the recommended approach utilizing the Kerberos protocol. The results of applying the recommended strategy are shown and discussed in Section 5. A definitive conclusion is reached in Section 6.

2. Related Works

The security of client authentication procedures is greatly increased by integrating smart cards into the conventional Kerberos protocol [8]. This enhancement is made possible via dual-factor authentication, which combines the user's possession (the smart card) with something they know (a password), and by safely keeping cryptographic keys within the smart card. Due to the dual-factor approach's requirement for both the smart card's ownership and accurate user credential input, it significantly lowers the danger of unauthorized access and offers a strong defense against a variety of security risks. This approach is based on a number of important research. Smart card technology and Kerberos work well together to offer a more robust security framework, as evidenced by research on safe authentication. It has been demonstrated that this strategy successfully mitigates typical vulnerabilities related to single-factor authentication. Strong cryptographic approaches are also essential for maintaining the secrecy and integrity of sensitive financial data both during transmission and storage, as research in encryption have shown. The cryptographic keys are handled and used securely thanks to the use of various encryption techniques inside the Kerberos framework [22]-[24].

- **Kerberos Protocol and Authentication:** Several investigations have been conducted on the Kerberos protocol as a reliable method for safe authentication in networked contexts. Neuman and Ts'o's landmark work, "Kerberos: An Authentication Service for Computer Networks," which describes how the protocol may offer safe identity verification via a reliable third-party Key Distribution Center (KDC), has had a significant impact [9]. This groundbreaking study emphasizes how well the protocol works to prevent unwanted access and how versatile it is for use in a range of security-sensitive situations. Md Mehedi Hasan et al. [10] employed IoT and end-user services for electrical service providers in smart grid applications. Source and destination authentication is needed for machine integration and AMI devices. Numerous protocols demand system development calculation time and communicational bit operations to identify two parties. Kerberos-based mutual authentication methods using elliptic curve cryptography decreased time and bit operations. Popular utility AVISPA researched protocols to comprehend and verify mutual authentication without understanding. Security and performance evaluations indicated this protocol delivered data quicker and with fewer bits than current systems.
- **Electronic Payment Security:** Numerous studies have been conducted on the security issues related to electronic payments. The use of authentication procedures and encryption are only two of the methods for protecting digital transactions covered in the study "Security of Electronic Payment Transactions" by Kousaridas et al. [11]. This paper supports the goals of the suggested Kerberos technique by highlighting the significance of putting strong security mechanisms in place in payment systems.
- **Kerberos in Financial Applications:** Research such as "Secure Mobile Payment Systems Based on Kerberos", Zhou et al. [12] investigated the use of the Kerberos protocol in financial transactions. This study highlights the benefits and

viability of incorporating Kerberos into mobile payment systems, especially in terms of boosting security by guaranteeing transaction integrity and user identity verification.

- **Symmetric Encryption in Payment Systems:** A crucial part of the Kerberos protocol, symmetric encryption is well known for its ability to safeguard private financial information. Researchers analyze the benefits and drawbacks of symmetric key cryptography in "Symmetric Encryption for Secure Transactions in Financial Systems," including information pertinent to the suggested method's dependency on Kerberos [13]. The study attests to the continued importance of symmetric encryption in safe electronic payments, particularly when paired with reliable authentication methods. Patel et al. [14] focused their attention on the significance of trust, security measures, and technologies that control the manner in which transactions take place in contactless payment cards and mobile wallets that are integrated with NFC. When it comes to increasing the safety and privacy of contactless payments, it is also important to analyze the EMV and ISO standards for contactless payment and to highlight the shortcomings of these standards. The fact that enemies might utilize these disputes to undermine the integrity of open connections is one of the reasons why they are troublesome.
- **Key Distribution and Trust Management:** For instance, Abdalzaher et al. [15] illuminate the significance of these processes and their primary efforts in the literature. We begin by addressing the primary intelligent assaults against SGs. Second, cryptography basics are covered. In the third section, we review typical key-management approaches and provide an evaluation of their benefits and downsides. Fourth, we introduce current authentication paradigms. Fifth, two typical mechanisms for checking protocol security and integrity are discussed. The research problems for trusting smart grids and protecting them from attacks and unauthorized entities are addressed in the sixth section with a future vision.

These connected publications serve as the suggested method's fundamental theoretical and practical cornerstones, highlighting its importance and approving its methodology. They offer strong proof of the applicability and efficacy of using the Kerberos encryption protocol to strengthen the security of electronic payment systems by drawing on a wealth of research.

Kerberos Protocol

Greek mythology depicts Kerberos [16], a three-headed hound guarding the underworld door. MIT created Kerberos, a network authentication system, as part of the Athena project in the mid-1980s. Kerberos uses secret-key cryptography to enable robust authentication for client/server applications. Kerberos still requires user credentials for identity verification. Credential exchange is secured throughout the authentication procedure, ensuring safe authentication. From the user perspective, it is similar to a typical sign-on process. The main distinction is that a temporary ticket is supplied to the client with verified identification. This ticket grants access to systems and applications within the Kerberos domain. Microsoft made Kerberos the default authentication system for corporate contexts with Windows 2000. All Windows 2000, XP, and Server 2003 OS platforms have a client Kerberos authentication provider. Kerberos implementation follows the IETF standard RFC 4120, which uses symmetric cryptography. Kerberos offers speedier authentication, mutual authentication, delegated access control, privacy, and data integrity through its unique ticketing system. Kerberos supports smart card login and single sign on (SSO) [17]. One benefit of Kerberos over alternative authentication protocols is that the password is never sent over the network, even when encrypted, and is encrypted/decrypted on the client workstation memory. Kerberos does not rely on firewalls as it does not consider intruder attacks. Kerberos involves three entities: the client, server, and Key Distribution Center (KDC), which consists of two services: the Authentication Service (AS) and the Ticket-Granting Service (TGS). The AS grants Ticket Granting Tickets (TGTs) to authenticated principals (users, computers, services) for TGS access. Tickets from the TGS provide access to other services inside the domain or to a trusted TGS in another domain. Any domain controller can handle authentication and ticket-granting requests sent to the KDC. Kerberos is a ticket-based system. Consider the following essential exchange scenario to understand how TGTs and service tickets work [18], [19]:

1. A consumer transmits a TGT request to KDC. The client's login but not password is in the request to generate their key.
2. The KDC delivers a TGT reply message with an encrypted session key to the client. The KDC encrypts its database-stored session key using the client's password. The KDC gives the TGS a ticket.

3. The client decrypts and extracts the session key from the encrypted reply message. Clients request service tickets. Only client and server communication are valid with a service ticket. Register the server with KDC.
4. The KDC generates a server service ticket. The ticket contains client authentication and a new sub-session key. The KDC encrypts the service ticket using the server-KDC secret key. Thus, only the server can decrypt the service ticket. The encrypted message encrypts the client copy of the sub-session key with the session key from the previous message.
5. The client decrypts the KDC message and extracts the sub-session key and service ticket. The server receives the service ticket.
6. The server decrypts the service ticket to get the client's authentication data and sector key. The server grants the client's request and starts a secure session. The client and server share a sub-session key for secure communication.

3. Proposed Method

The strong authentication and key management capabilities of the Kerberos encryption protocol are used in the suggested solution to strengthen the security of electronic payments. This method assures safe communication between consumers and financial institutions by utilizing a trustworthy Key Distribution Center (KDC) and symmetric encryption. By using smart cards, the technique also facilitates dual-factor authentication, enhancing identity verification and preventing unwanted access to private financial information. The objective of this approach is to offer an effective, safe framework for protecting electronic payments in the current, increasingly digital economy. The graphic below provides an overview of the suggested method's chart.

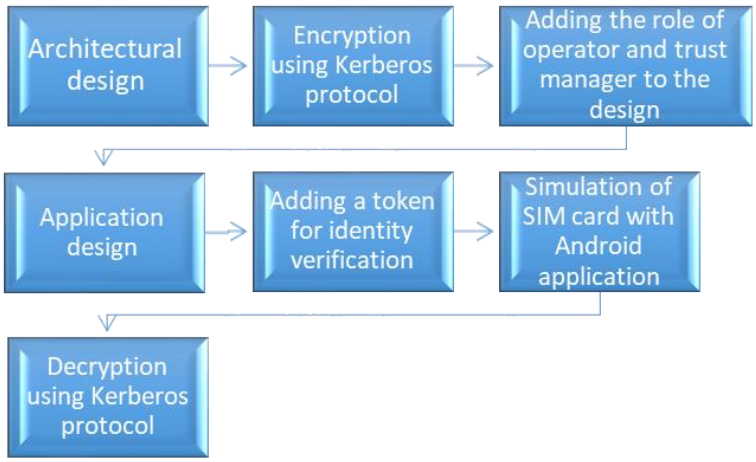


Figure 1. The Proposed Method

The architecture for the suggested mobile payment system is divided into four stages:

1. Agreement and announcement phase
2. Loyalty points collection and conversion to a mobile coupon
3. Coupon usage phase
4. Account settlement phase

The procedure also includes four crucial roles:

1. Suppliers
2. Mobile Coupon Service Provider (MCSP)
3. Retailers
4. Customers (MCSP members)

Let's utilize a trust manager in this study to protect mobile coupons. In this sense, the SIM card serves as the trust manager's server and is considered the third party. Thus, we store the keys in the SIM card and see it as a secure module. Retailers and consumers do not produce their own shared keys while using the shared key method; instead, they obtain them from the operator. The Trust Manager is responsible for the following tasks:

- Key production
- Key distribution
- Resolving differences

A mechanism for collecting loyalty points, turning them into mobile vouchers, and using them in different ways is part of the original idea. A horizontal and vertical hash chain are used to create loyalty points. The primary chain is mirrored by the upper horizontal chain. Given n clients and a maximum of 20 loyalty points per transaction, the number of customers is subjected to the initial hash function on the generator value, w0, which is represented by the first row of the matrix. The method proceeds to the vertical sub-chains after the primary horizontal sub-chain is finished, using a secondary hash function hierarchically along the vertical levels. A row from the matrix's columns is assigned to a customer with each successful transaction, and this row has to be communicated to the appropriate customer. Thus, the suggested methodology is divided into three phases:

1. Identity verification
2. Matrix implementation
3. Application design

The client application's user interface is displayed in the following figure:

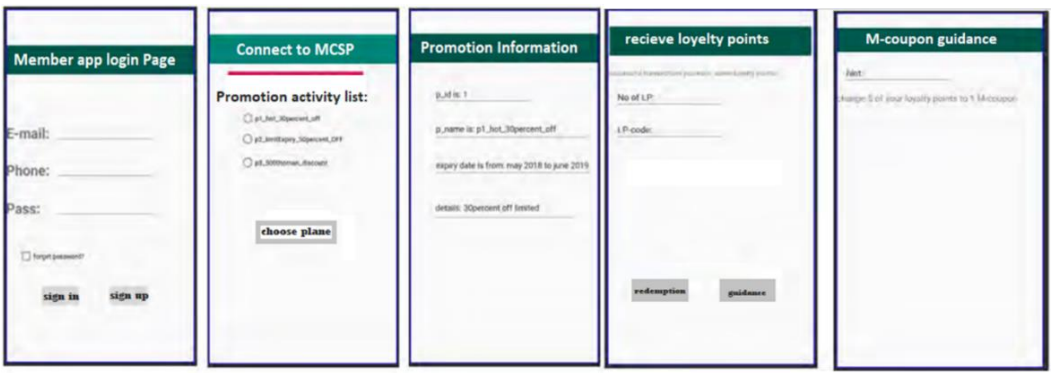


Figure 2. Client application's user interface

The merchant application's graphical interface is depicted in the following figure:

Figure 3. Application's graphical interface

Our approach makes use of Trust Manager, a third-party service that offers an authentication token. For safe identification verification, a 74-bit random string is issued to each user. Only the hashed text is delivered when a request is made to the mobile coupon server. In order to verify the user's identity, the server searches the database for the string. By using a shared key between the sender and the recipient, eavesdroppers are prevented from using the entire key, even if it is intercepted. The Kerberos protocol, which utilizes symmetric key encryption for secure authentication, handles decryption in the mobile coupons system. All network clients' and servers' private keys are kept at the Key Distribution Center (KDC) and are used for information sharing. Kerberos generates a temporary session key for interaction among clients, servers, and the KDC through the Ticket Granting Service (TGS), ensuring secure interactions.

4. Experimental Results

The Python web framework in Python was employed to develop a mobile coupon service provider in this study. Additionally, Android Studio was employed to construct two retail Android applications and a customer application. Python was used to implement the X matrix on the server side, while Java was used to design the retail application. In order to conduct experimentation and analysis, a variety of factors were investigated, such as the computational complexity, customer loyalty after security was guaranteed, mobile coupon issuance, and coupon subscription, as well as the time costs associated with dispatch and operations. Furthermore, comparisons were conducted with comparable mobile coupon architectures, utilizing findings from investigations by [20], [21].

The results of this research are presented in comparison to previous protocols, and the analysis method is comparative. In previous systems, users requested a shared key or token from the mobile coupon service provider, which issued a one-time password after authenticating the username and password. This method was susceptible to assaults. Nevertheless, the protocol that has been suggested in this investigation is significantly different. A shared key is requested by the user from the mobile coupon server via the operator, and tokens are exchanged between the user and the operator. This guarantees that the operator can confirm the legitimate proprietor of the authenticated SIM card. The proposed protocol implements authentication at the mobile operator network level, in contrast to the reference study (Chin et al., 2017), which utilized columns as safeguards by summing them in the matrix. This research facilitates encryption by eliminating the public key and integrating a token system through an API, in contrast to the previous system, which utilized public and private keys for components (see Figure 4). The operator is now a component of the token cycle, assuring a more secure coupon payment system that is based on SIM card authentication, despite the fact that token exchange occurs between two members. The greatest number of characters that could be found on the keys that the operator generated for this study was 74. The amount of our data is 18,432 bits, which is equivalent to 4,608 bytes and, consequently, 25.2 kilobytes. This is due to the fact that each character is represented by 32 bits, and each key exchange requires nine key exchanges. It is possible to determine the transmitting time by calculating the total response times of all HTTP requests (see Figure 5).

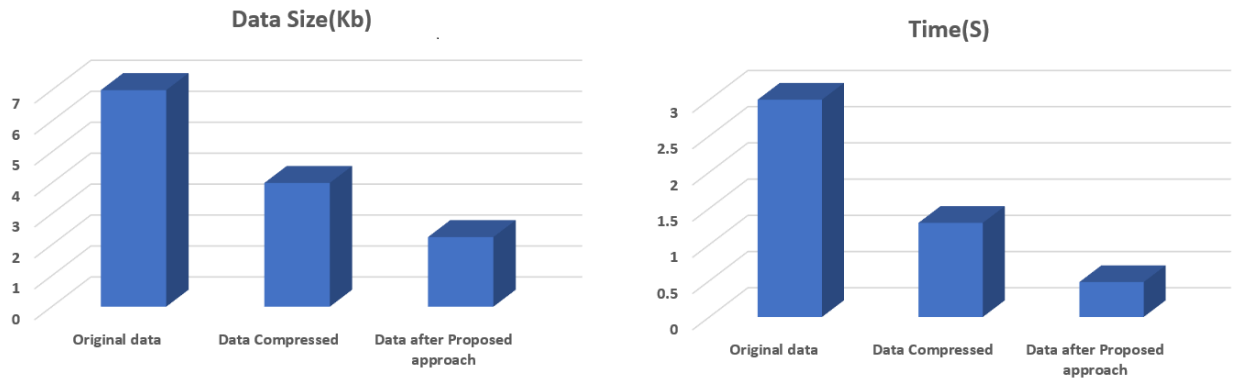
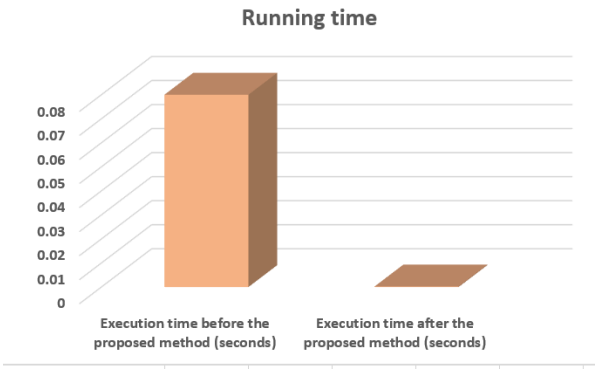


Figure 4. Performance the proposed method



(A) (B)

Figure 5. Comparison Performance on smartphones of proposed method(a) One-way hash function (b) verify function

Table. 1 Compared to comparable mobile coupon architects

Architecture	Supervision	Coupon Subscription	Coupon Use	Coupon Issuance	Earn Loyalty Points
Hsueh Architecture (Sueh et al. 2017) [20]	No	Yes	Yes	Yes	No
Chen architecture (Chen et al. 2017) [21]	No	No	Yes	Yes	Yes
Proposed architecture	Yes	No	Yes	Yes	Yes

5. Conclusions and Future Work

Materials on electronic commerce and suitable ways to establish a foundation of trust with customers and conduct financial transactions via mobile devices were provided in this study. In order to improve security and foster consumer confidence in mobile-based banking transactions, this study investigates potential solutions. It emphasizes how crucial it is to have e-commerce infrastructure in order to manage risks and stay up to date with international markets. Businesses may boost confidence and guarantee a secure mobile payment experience by putting security measures in place, controlling risks, and integrating secure solutions. In further work, we may employ a variety of safe stream cipher techniques to guarantee the security of the encrypted data.

References

[1] N. Singh, “Impact of e-banking: Prior and after effects on banking activities,” *Journal of Pharmaceutical Negative Results*, pp. 310–317, 2023.

[2] A. T. Oyewole, C. C. Okoye, O. C. Ofodile, and C. E. Ugochukwu, “Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio,” *World Journal of Advanced Research and Reviews*, vol. 21, no. 3, pp. 625–643, 2024.

[3] H. Akbar, M. Zubair, and M. S. Malik, “The security issues and challenges in cloud computing,” *International Journal for Electronic Crime Investigation*, vol. 7, no. 1, pp. 13–32, 2023.

[4] E. E. Archibong, B. U.-A. Stephen, and P. Asuquo, “Analysis of Cybersecurity Vulnerabilities in Mobile Payment Applications,” *Archives of Advanced Engineering Science*, pp. 1–12, 2024.

[5] T. Wang, T. Liu, and H. Zhu, "Cybersecurity Challenges in Mobile Payment Systems: A Case Study of Alipay in Chinese Cities," *Innovation in Science and Technology*, vol. 3, no. 1, pp. 51–58, 2024.

[6] A. Mohamed, "Intelligent Blockchain-Based Secure Framework for Transaction in Mobile Electronic Payment System.," *International Journal of Interactive Mobile Technologies*, vol. 17, no. 4, 2023.

[7] M. Sinha, H. Majra, J. Hutchins, and R. Saxena, "Mobile payments in India: the privacy factor," *International Journal of Bank Marketing*, vol. 37, no. 1, pp. 192–209, 2019.

[8] I. Downnard, "Public-key cryptography extensions into Kerberos," *IEEE Potentials*, vol. 21, no. 5, pp. 30–34, 2003.

[9] B. C. Neuman and T. Ts'o, "Kerberos: An authentication service for computer networks," *IEEE Communications magazine*, vol. 32, no. 9, pp. 33–38, 1994.

[10] M. M. Hasan, N. A. M. Ariffin, and N. F. M. Sani, "Efficient mutual authentication using Kerberos for resource constraint smart meter in advanced metering infrastructure," *Journal of Intelligent Systems*, vol. 32, no. 1, p. 20210095, 2023.

[11] A. Kousaridas, G. Parissis, and T. Apostolopoulos, "An open financial services architecture based on the use of intelligent mobile devices," *Electronic Commerce Research and Applications*, vol. 7, no. 2, pp. 232–246, 2008.

[12] S. Zhou, Y., Tang, Y., & Li, "Secure Mobile Payment Systems Based on Kerberos," *International Journal of Computer Science and Network Security*, vol. 11, no. 9, pp. 1–7, 2011.

[13] R. L. Rivest, "Symmetric Encryption for Secure Transactions in Financial Systems," *Journal of Cryptography*, vol. 1, no. 1, pp. 21–33, 1990.

[14] Y. Patel, N. Chovatia, and H. Kaur, "Securing Payment Transactions: A Comprehensive Review of Smart Cards and Contactless Payments with Cryptographic Methods," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2024, pp. 785–790.

[15] M. S. Abdalzaher, M. M. Fouda, A. Emran, Z. M. Fadlullah, and M. I. Ibrahem, "A survey on key management and authentication approaches in smart metering systems," *Energies*, vol. 16, no. 5, p. 2355, 2023.

[16] M. Shagam and E. Ronen, "Windows into the Past: Exploiting Legacy Crypto in Modern {OS's} Kerberos Implementation," in *33rd USENIX Security Symposium (USENIX Security 24)*, 2024, pp. 6651–6668.

[17] W. Lazarov, A. Bohacik, D. Kohout, and R. Fujdiak, "Training Scenario for Security Testing of the Kerberos Protocol," in *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*, 2024, pp. 56–67.

[18] J. Gong, T. Men, S. Feng, and D. Yu, "An Analysis and Improvement Scheme for the Weakness of Kerberos V5 Authentication," *Journal of Electrical Systems*, vol. 20, no. 2, pp. 1955–1960, 2024.

[19] Y. Begimbayeva, Z. Ospanov, L. Gorlov, R. Ibrayev, and O. Ussatova, "Approaches to Developing Key Distribution Protocols Based on Quantum Key Distribution," *Journal of Electrical Systems*, vol. 20, no. 7s, pp. 2323–2330, 2024.

[20] Z. Qin, J. Sun, A. Wahaballa, W. Zheng, H. Xiong, and Z. Qin, "A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing," *Computer Standards & Interfaces*, vol. 54, pp. 55–60, 2017.

[21] Y.-Y. Chen, M.-L. Tsai, and F.-J. Chang, "The design of secure mobile coupon mechanism with the implementation for NFC smartphones," *Computers & Electrical Engineering*, vol. 59, pp. 204–217, 2017.

[22] Hayder Talib Jawad Al-Sammak "Propose an Object Detection Optimization Algorithm by Using Particle Swarm Optimization (PSO) Based-on Exploration Ability of Grey Wolf Optimizer (GWO)", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 5, Issue 2, pp. 54-60, 2024.

[23] Mohammed Fareed Mahdi "Revolutionizing the Future Investigating the Role of Smart Devices In IOT", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 5, Issue 1, pp. 1-15, 2024.

[24] Rohini Pochhi, Sandeep Thakre, Balwant Bansod "Using wireless sensor network for monitoring and controlling of farm", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 2, issue 1, pp. 22-25, 2021.

[25] Samyak S. Nagrare, Payal N. Kanchanwar, Prashant V. Patle, Varsha V. Ambule"Real-Time Smart Face Security Estimation", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 2, issue 2, pp. 18-23, 2021.

[26] Sanjana Awachat, Ashwini Chahande, Sakshi Gadge, Snehal Shastrakar, Karishma Gajbhiye"A Secure Cloud Based Chatting Application with Hybrid Cryptography", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 2, issue 2, pp. 42-45, 2021.