SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 5141-5150
Open Access. Online & Print

DOI: 10.5281/zenodo.19113849

TOUCHLESS MULTI-FACTOR AUTHENTICATION FOR HOSPITAL INFRASTRUCTURE USING SMART CARDS AND CARDIO-BIOMETRIC SIGNALS

Nuha Lutfi*†[1], Sarun Puthanpurayil Kaliyarmban*†[2], Kashif Aziz*†[3], Abdul Aziz Abdul Qader*†[4], Mohammed Abdul Haq Mujahed*†[5], Mohamed Izeldin Siddig Malik*†[6], Shigul Thundiyil*†[7], Syed Muhammad Ali Haider*†[8], Aya Ahmad Khaleel Abuhmaid*†[9]

[1]Independent Researcher, Saudi Arabia, Email: nuha.ibrahim.lutfi@gmail.com
[2]Independent Researcher, Saudi Arabia, Email: sarunpk@gmail.com
[3]Independent Researcher, Saudi Arabia, Email: kashifaziz007@hotmail.com
[4]Independent Researcher, Saudi Arabia, Email: abdul1913aziz@gmail.com
[5]Independent Researcher, Saudi Arabia, Email: abdulhaq333@gmail.com
[6]Independent Researcher, Saudi Arabia, Email: mohdezzealdenmalik@hotmail.com
[7]Independent Researcher, Saudi Arabia, Email: shigul.t@gmail.com
[8]Independent Researcher, Saudi Arabia, Email: smali_system@yahoo.com
[9]Independent Researcher, Saudi Arabia, Email: aya.ahmad11@live.com
† These authors contributed equally to this work

Received: 06/02/2026
Accepted: 05/03/2026

Corresponding Author: All authors are corresponding authors (nuha.ibrahim.lutfi@gmail.com; sarunpk@gmail.com; kashifaziz007@hotmail.com; abdul1913aziz@gmail.com; abdulhaq333@gmail.com; mohdezzealdenmalik@hotmail.com; shigul.t@gmail.com; smali_system@yahoo.com; aya.ahmad11@live.com)

ABSTRACT

As hospitals increasingly adopt digital infrastructures, security, efficiency, and cleanliness have become major factors in choosing authentication systems. Common methods such as passwords, PINs, and fingerprint scanners are still subject to the same limitations of usability, hygiene, and security when applied in healthcare. Among these approaches, MFA stands out as the most secure, as it requires validating a user's identity with more than one factor. However, the current technical implementations are lacking when it comes to operation without touching surfaces or working through the time restrictions of hospital environments. The present research investigates the use of touchless multi-factor authentication for hospital infrastructure through the pairing of smart cards as a means of possession factor with cardio-biometric signals as a physiological biometric factor. This study examines the use of smart cards for staff identification and access, the feasibility of cardio-biometric signals for liveness-aware authentication, and the development of secure, user-friendly, and privacy-preserving technology through appropriate design considerations. This paper presents and discusses the system architecture, authentication workflow, and practical considerations for deployment in clinical settings. The main contribution of this research is filling a void in the existing literature on hospital authentication systems by introducing a carefully structured framework that merges touchless interaction,

high-assurance authentication, and healthcare-specific usability needs. This project lays down a conceptual basis from which secure, large-scale, and hygienic authentication solutions can be developed, thus facilitating both theoretical comprehension and real-world applications in contemporary hospital settings.

KEYWORDS: Multi-Factor Authentication; Touchless Authentication; Hospital Infrastructure; Smart Cards; Cardio-Biometric Signals; Healthcare Security; Biometric Authentication.

1. INTRODUCTION

The swift digitalization of healthcare infrastructure has led to a complete change in hospital operations, more efficient management of patient data, clinical workflows, and access-controlled facilities. Hospitals are increasingly interlinked with information systems and smart technologies that facilitate medical decision-making and patient care. These advancements, while certainly very positive, not only enhance the efficiency of operations and quality of care but also increase the risk of unauthorized access, data breaches, and identity fraud. Thus, it goes without saying that strong authentication mechanisms are inevitable to protect patients' safety and support healthcare professionals' access to clinical systems and secure areas, thus ensuring compliance with regulations. Authentication is the procedure of asserting a person's identity before granting access to digital or physical resources. Conventional authentication practices in healthcare settings mainly depend on knowledge-based credentials, such as passwords and PINs, or touchless biometric systems, such as fingerprint and palm scanners. However, these techniques have significant drawbacks when used in clinics. Knowledge-based credentials can be lost through unauthorized access, reuse, or social engineering attacks, while contact-based biometric systems can raise hygiene concerns and slow down workflows, particularly when healthcare staff need to wear personal protective equipment (PPE) or require quick access during emergencies. In the era of the Internet of Healthcare Things (IoHT), authentication solutions must be more advanced and match the evolving threats and operational needs of healthcare providers, thus enhancing the necessity for multi-factor authentication. (MFA) (Suleski et al., 2023). Multi-Factor Authentication utilizes a series of independent proof factors that are usually grouped as knowledge (something the user knows), possession (something the user has), and biometric (something the user is) to increase the reliability of authentication and lower the risk of unauthorized access. The use of MFA has been the subject of extensive research as a security measure in various areas, such as cloud computing and critical infrastructure, with results showing that the methods have become more resistant to impersonation and credential compromise (Ganmati et al., 2025). However, existing MFA systems are not often tailored to the specific needs of medical environments, where no-touch, clean, and smooth solutions are progressively required. Smart cards, among the possession-based factors, have been used in the medical sector to handle the identities of workers and provide access to restricted areas because of their ability to securely store information and perform cryptographic operations. However, if smart cards are used alone, there is still a risk, for example, of losing the card or sharing the card, which means that the use of additional authentication factors is necessary to achieve a higher level of assurance. Biometric authentication provides a support security level with the most common methods, which are based on the use of physiological characteristics that are difficult to copy or forge. Newer biometric methods, especially cardiovascular signals such as electrocardiogram (ECG) and photoplethysmography (PPG), have shown their capability for safe and liveness-aware authentication in medical and IoHT situations, with the coming together of different modalities proving to have better accuracy and being more resistant to spoofing (Ahamed et al., 2022). Although there have been advancements in the fields of smart cards and biometrics, the adoption of touchless MFA systems that merge smart cards with heart biometrics has not yet been explored in the field of health research. This unoccupied area has led to speculation as to what extent these combined touchless authentication systems adhere to both the strictest security measures and the practical difficulties of the hospital setting.

2. BACKGROUND AND RELATED WORK

Authentication is a very important step in the process of keeping hospitals' digital and physical assets safe, where sensitive patient information and restricted access areas must be controlled. Hospitals, as well as other sectors, have relied on traditional single-factor authentication, such as passwords or personal identification numbers (PINs), because they are very simple and do not require a lot of time or resources for implementation. Despite that, it is still the case that single-factor authentication is not sufficient for such environments that have very strict security requirements. The two-factor authentication that combines a knowledge factor with either an ownership or biometric factor, on the other hand, has been able to add a significant layer of security through verification. In the healthcare sector, two-factor methods dependent on touch-based biometrics can slow down the workflow and efficiency in the case where the staff is required to wear personal protective equipment (PPE) or needs quick access to several systems (Vale et al., 2022). The use of multi-factor authentication (MFA), which combines knowledge, ownership,

and biometric factors, provides a very secure model and has been adopted in banking and critical infrastructure (Ganmati et al., 2025). Despite these developments, traditional MFA systems are seldom configured for touchless operation, which is a requirement in healthcare to maintain hygiene and reduce the risk of contamination. Hospitals offer very different authentication challenges: the medical team must easily access systems and places with limited entry without endangering patient safety or being a nuisance to the workflow. Fingerprint and keypad systems rank hygiene lowest among the factors and are difficult to use in sterile places or during emergencies. Although there are non-contact biometric methods, such as iris and facial recognition, that can be implemented in the healthcare sector, their performance can be easily outweighed by environmental conditions, the use of PPE, and user compliance (Vale et al., 2022). In hospitals, smart cards have become a dependable authentication method based on ownership. Smart cards, which store encrypted user credentials and enable contactless verification through RFID or NFC technologies, grant medical personnel access to e-health records, restricted zones, and non-contact operation of medical equipment. However, smart cards, by improving the user experience and supporting the practice of 'no-contact' procedures, are still prone to certain security issues, such as theft, loss, or unintentional sharing. Therefore, the security of the system can be significantly improved by introducing biometric factors along with smart cards. Cardiobiometric signals, such as electrocardiography (ECG) and photoplethysmography (PPG), offer a physiological perspective for identification, as they reveal distinctive patterns of heart activity. These signs can be gathered without the person having to be present, thus providing liveness detection and the possibility of continuous verification of medical personnel (Ahamed et al., 2022). The endorsement of cardio-biometrics as a key authentication technology in clinical settings has been growing, despite the hurdles of movement or stress causing signal variations, the necessity for precise sensors, and careful data management. Simultaneously, the combination of ownership elements and biometrics has been investigated with applications in finance and government; however, the combination of smart cards and cardio-biometrics for non-contact multi-factor authentication in clinics has been left mostly unexplored. Current hospital systems use either touch biometrics or smart cards but never both, resulting in a significant gap in research. This gap needs to be addressed to develop authentication systems that provide security, are hygienic, facilitate clinical workflows, and comply with privacy regulations. The present study aims to improve this neglected area by suggesting a no-touch MFA framework that fits into the hospital infrastructure, where smart cards and cardio-biometric signals would come together to create strong, hygienic, and productive authentication for healthcare professionals.

3. AUTHENTICATION PROCESS AND WORKFLOW

The workflow of a contactless multi-factor authentication system in hospitals is constructed in such a way that it not only supports clinical activities but also secures and hygienically maintains the environment. The first step is the enrollment of healthcare professionals in the system. At this point, the person receives a non-contact smart card that keeps their identity credentials encrypted, and at the same time, the person’s bio-signal is captured. ECG or PPG is captured using non-invasive sensors, and a secure biometric template is created by extracting unique features (Ahamed et al., 2022). This template is linked to the smart card credentials, and using privacy-preserving encryption, the hospital authentication server stores it in such a way that it cannot be accessed or leaked due to the security measures taken against unauthorized access or sensitive physiological data being leaked (Nguyen et al., 2020).

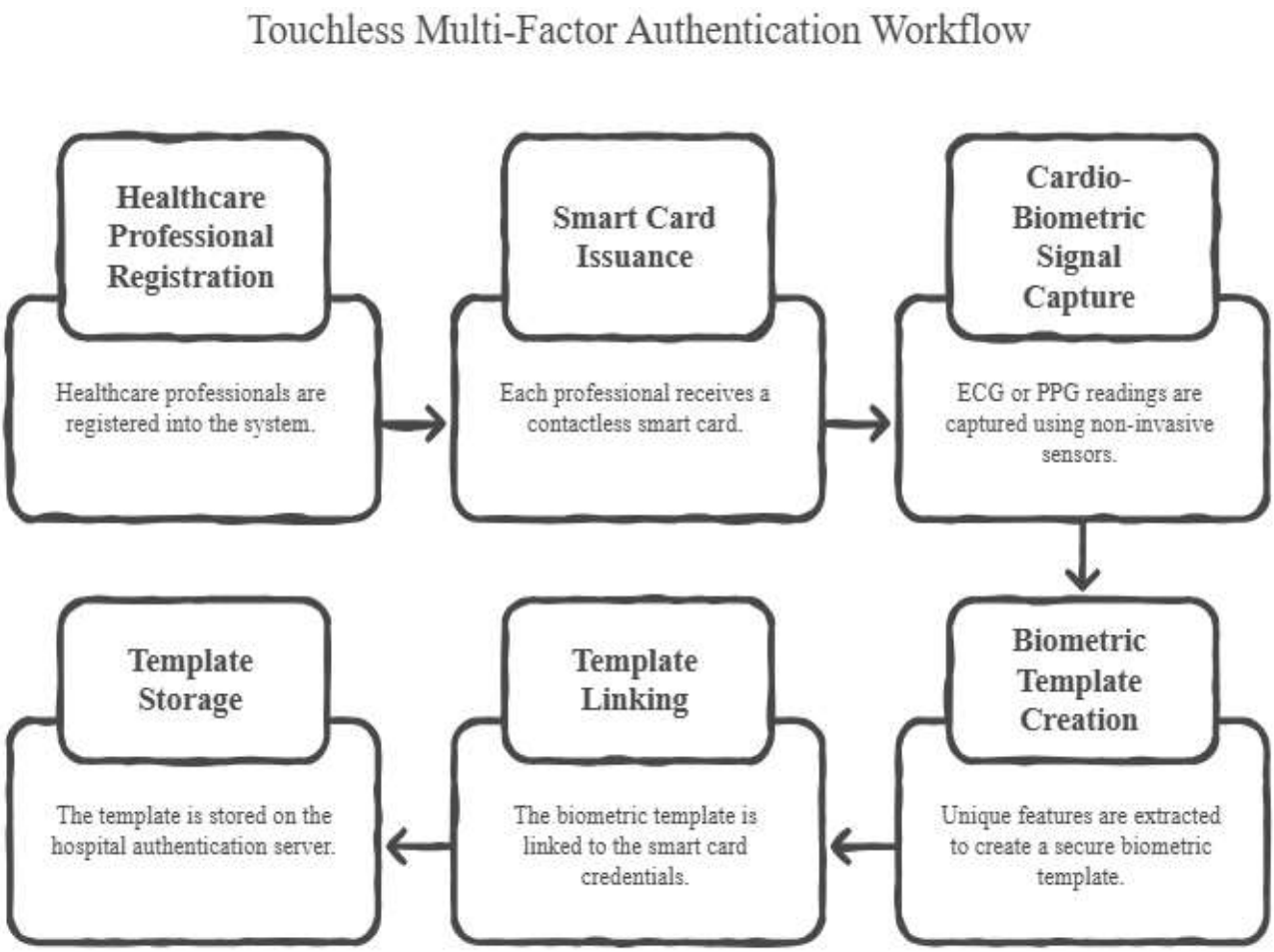

Figure 1: Touchless Multi-Factor Authentication Workflow.

Enrolling comes first, and the verification phase occurs every time a staff member wants to enter a restricted area or use a restricted system. After the smart card is shown to the contactless reader, the system initiates a secure handshake with the card to obtain the encrypted ownership credentials. Simultaneously, the cardio-biometric sensor acquires a live physiological signal from the person without the need for physical contact. Then, the advanced signal processing algorithms pick out the relevant features of the heart, and these are compared with the stored template to find a match. The system applies adjustable decision thresholds to cater to the natural variability of cardiac signals while achieving high accuracy and maintaining low false acceptance and rejection rates (Gao et al., 2021). The access decision is the product of combining the results of the ownership and biometric factors. The system allows access only after both factors are successfully verified, thus providing a high level of authentication assurance. In cases where biometric verification fails because of temporary anomalies or sensor malfunctions, an alternative knowledge factor, such as a secure PIN, could allow limited emergency access as a last resort, and would thus maintain operational continuity with no security compromise (Vale et al., 2022). In conclusion, every authentication event is documented in an audit log that serves monitoring and compliance purposes. This practice enables hospital supervisors to recognize access trends, pinpoint questionable activities, and compile reports to adhere to regulations. By linking enrollment, authentication, and logging into a smooth workflow, the suggested system ensures that contactless multi-factor authentication is both convenient for daily hospital activities and strong against security threats (Ometov et al., 2018).

4. CARDIO-BIOMETRIC SIGNAL PROCESSING AND MATCHING

Authentication using cardio-biometry is based on the individual's heart activity, which is unique to him/her and can be detected using methods such as electrocardiography (ECG) or photoplethysmography (PPG). The signals have a very high assurance of authentication, as they

possess several inherent advantages, such as liveness detection and resistance to reproduction or forgery (Ahamed et al., 2022). Nevertheless, the effective application of cardio-biometric data in a hospital context is difficult unless signal acquisition, preprocessing, feature extraction, and matching are carefully performed to accommodate the dynamic environment and variances in the physiological states of the staff. Signal acquisition may be performed through wearable devices or ambient sensors that are strategically positioned to obtain cardiac signals without any physical contact, thus maintaining hygiene in a clinical setting. ECG traces, for example, show the electrical activity of the heart, while PPG indicates changes in blood flow volume, both producing patterns that are unique to each person (Nguyen et al., 2020). The unprocessed signals frequently have noise from different sources, such as a person's movement, the muscles around the sensor, or the electrical activity in the environment. Hence, preprocessing techniques such as bandpass filtering, baseline correction, and motion artifact removal are necessary for good signal quality and reliability (Gao et al., 2021). After preprocessing, relevant features are extracted to form a biometric template. The most common features include the time intervals between heartbeats, variations in amplitude, and shapes of ECG waveforms or PPG pulses. These features provide a compact and discriminative representation of a person's heart signature (Ahamed et al., 2022). Machine learning models or statistical classifiers can then be used to match the incoming signals against the stored templates, considering the intra-user variability caused by stress, physical activity, or health conditions. Adaptive thresholding and continuous template updates make it possible to improve accuracy while reducing the rates of false acceptances and false rejections (Vale et al., 2022). The last conclusion combines the outcomes of cardio-biometric matching with ownership confirmation from the smart card. This combination guarantees that both methods of authentication, something you have "something you have" and "something you are" are validated simultaneously, making it a very strong authentication process that is suitable for sensitive hospital environments (Ometov et al., 2018). The cardio-biometric signals that would support smart card authentication with great reliability are those resulting from careful signal processing, secure template storage, and adaptive matching techniques, thus allowing the creation of a practical, touchless multi-factor system that provides both security and operational efficiency.

5. PRIVACY, SECURITY, AND COMPLIANCE CONSIDERATIONS

The deployment of touchless multi-factor authentication (MFA) into hospital infrastructure raises important privacy and security issues, as sensitive personal, physiological, and institutional data are processed and stored all the time. Cardio-biometric signals, while providing a high level of confidence, are still treated as personally identifiable and health-related information. Hence, it is imperative to take strong action to guarantee that data collection, storage, transmission, and processing are in accordance with legal regulations and ethical standards (Nguyen et al., 2020; Ahamed et al., 2022). The safeguarding of biometric templates is one of the basic foundations on which security is built. The system should not only hold the ECG or PPG signals, but also draw discriminative features from them and encode them in templates that are sufficiently secure, preferably through a one-way transformation or encryption scheme. The use of methods such as template hashing or homomorphic encryption can make it impossible for attackers to recreate the original cardiac signals, thus reducing the chances of identity theft or unauthorized cloning (Gao et al., 2021). In addition, the system should create secure communication paths between smart card readers, biometric sensors, and authentication servers using protocols such as Transport Layer Security (TLS) to block interception or replay attacks. Another main point is user consent and minimization of data. Hospitals must set policies that enable personnel to be aware of the data being gathered, how it is handled, and for what reasons it is used. Keeping data for the shortest possible time reduces the risk of exposing it and makes the organization comply with regulations such as the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) (Vale et al., 2022). In addition, conducting audits and logging who accesses what are the main tools to determine potential breaches, keep track of unauthorized attempts, and provide the necessary information for compliance reporting. Moreover, operational policies should consider fallback and emergency situations, along with the security of the system. For example, if the capture of a cardio-biometric signal becomes unreliable because of a temporary health issue or a malfunctioning sensor, then an alternative method for authentication, such as a secure PIN or an emergency override, can be used. These mechanisms must be strictly controlled and supervised to avoid misuse (Ometov et al., 2018). By including high-end template protection, secure communication, data

minimization, and compliance-oriented auditing, the proposed touchless MFA system enables hospitals to use high-assurance authentication without sacrificing privacy or regulatory compliance. Such measures are necessary to maintain the trust of healthcare professionals and patients while protecting sensitive medical and identity data.

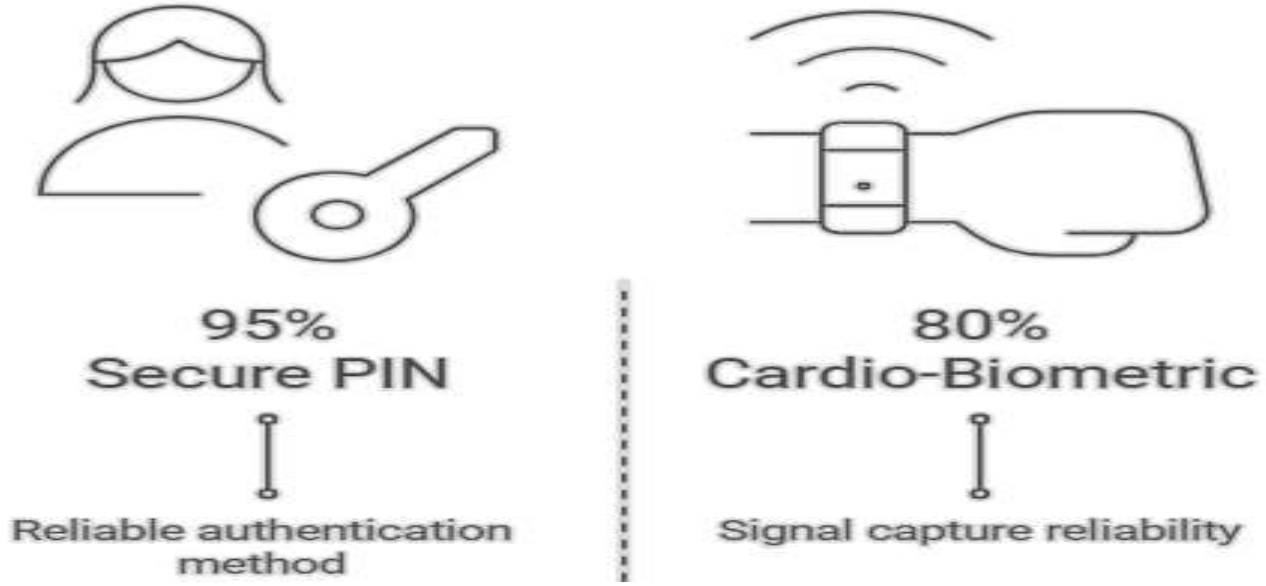

Figure 2: Authentication Method.

6. EVALUATION METHODOLOGY

The technical performance and practical usability of a touchless multi-factor authentication system for hospital infrastructure should be evaluated using a comprehensive and methodical approach. Evaluation metrics for authentication precision, system reliability, technology integration, and ability to withstand security attacks were included in the evaluation process, thus confirming that the solution is both efficient and practical for deployment in the real world (Ometov et al., 2018; Vale et al., 2022). The performance metrics were the false acceptance rate (FAR), false rejection rate (FRR), and overall authentication accuracy. The FAR indicates the likelihood of an unauthorized person being mistakenly granted access, whereas the FRR indicates how many times a lawful user has been denied access because of biometric inconsistency or system error. These metrics are more important in the case of cardio-biometric signals, which can be affected by different physiological conditions, such as stress, movement, or even the patient's health (Ahamed et al., 2022). Continuous evaluation performed over various sessions allows not only to test the intra-user consistency but also to determine the temporal stability of the authentication system. However, usability and workflow assessment is of utmost importance because medical staff in hospitals work in fast-moving and stressful situations. The evaluation considered the authentication speed, convenience of using touchless sensors, and influence on the clinical workflow. User feedback and task analysis can pinpoint possible bottlenecks, issues with sensor placement, or ergonomic challenges, ensuring that the authentication process does not interfere with patient care (Nguyen et al., 2020). The security analysis considers the most common threat vectors, such as credential theft, impersonation, replay attacks, and spoofing of cardio-biometric signals. Scenario-based attacks, penetration testing, and adversarial experiments can not only validate the resistance of the system but also identify the areas that require more protection, such as encryption, safe storage of templates, and multi-factor fusion strategies (Gao et al., 2021). Ultimately, the evaluation protocol incorporates a comparative study of the different existing authentication mechanisms, that is, password-based, card-only, or traditional two-factor systems. In this way, the comparison will be able to show the merits of touchless MFA, especially regarding hygiene, user-friendliness, and liveness-aware security. The combination of quantitative metrics and qualitative observations creates a holistic assessment of the system's suitability for deployment in hospitals (Vale et al., 2022).

7. DISCUSSION

One of the notable advantages to the implementation of touchless multi-factor authentication (MFA) in hospitals is the significant gain in patient privacy, still, on the other hand, there are obstacles that need to be evaluated thoroughly. The system integrates the use of smart cards as the ownership factor with cardio-biometric signals as the physiological factor, thereby addressing the major issues of security, hygiene, and usability, which are always associated with the healthcare workflow (Ometov et al., 2018; Vale et al., 2022). The major benefit is the security of the system, which is greatly enhanced by the combination of the two different authentication factors. Authorized sharing, theft, and loss are some of the ways smart cards are compromised; however, with the inclusion of cardio-biometric verification, only authorized personnel can access the area; hence, impersonation and fraudulent usage risks are significantly reduced (Gao et al., 2021). In addition, cardio-biometric signals are associated with liveness detection, which is a feature that prevents spoofing attacks that often occur in conventional biometric systems, such as fingerprints or facial recognition, where the systems are very vulnerable (Ahamed et al., 2022). Touchless technology used in authentication factors is an asset from a usability viewpoint, as it minimizes disruptions to hospital workflows. Hospital staff can quickly perform authentication without contact, reducing the chance of cross-contamination in sensitive clinical areas. This has even greater significance in already difficult situations where emergency rooms, intensive care units, or infectious disease wards are crowded and hygiene along with speedy access is the utmost concern (Nguyen et al., 2020). However, practical deployment also presents technical and operational challenges. A person's cardio-biometric signals may change if they are in a different physical condition, performing physical activity, or if the sensor is placed differently. This necessitates adaptive algorithms and excellent preprocessing methods to maintain the same level of accuracy (Ahamed et al., 2022). Integrating with current hospital information systems might require some alterations and take into account the issue of interoperability, which involves secure communication protocols and compliance with legal requirements such as HIPAA and GDPR (Vale et al., 2022). Another aspect that must be evaluated is the trade-off between security, cost, and complexity. On the one hand, the use of smart cards along with cardio-biometrics undoubtedly increases the security level; however, on the other hand, it involves buying sensors, server infrastructures, and maintenance, which also occupy a large part of the budget. Hospitals would need to weigh these costs against the operational and security advantages, and at the same time, ensure that the deployment is both scalable and sustainable. Overall, the proposed touchless MFA framework provides a convincing solution for authentication assurance elevation in hospitals. By behaving the same way with healthiness, security, and usability, it lays down the groundwork for the future acceptance of high-assurance, user-friendly authentication systems in healthcare environments (Ometov et al., 2018; Gao et al., 2021).

8. FUTURE RESEARCH DIRECTIONS

The creation of touchless multi-factor authentication (MFA) systems for hospital infrastructure, which will involve smart cards as well as cardio-biometric signals, is a major step towards future research geared at securing, easing, and scaling up processes in hospitals among other things, thereby opening up several avenues. One of the directions that arise from this is to check for continuous and adaptive authentication. The continuous monitoring of cardio-biometric signals can provide real-time assurance that the authenticated user is still present and is still authorized, thereby providing even more protection for sensitive hospital areas and systems over the traditional time-point verification, which usually involves stopping the process to authenticate or verify the user (Ahamed et al., 2022). Another area that can be focused on is AI-based signal processing and feature optimization. For example, the application of machine learning models will lead to the accuracy of the cardiac signal being identified to significantly increase, as they can consider the variations that are specific to the user over time, that is, they can compensate for physiological changes that occur due to stress, fatigue, or health conditions. In addition, AI can also dynamically adjust the decision thresholds, which would lead to a reduction in the number of false rejections but at the same time maintain a very low level of false acceptance, which is critical for high-paced healthcare environments (Gao et al., 2021). The clinical validation and actual use of touchless multi-factor authentication systems in different hospital environments should be the main focus of future studies. Although laboratory assessments or trials prove feasibility, longitudinal studies in operational healthcare settings will tell the story of the reliability, acceptance, and emergency performance of the system. The system's

investigation will include the how's and why's of cardio-biometric signals in high-stress clinical situations, such as surgery and emergency response, where physiological variability might impact the authentication accuracy. Along with the above considerations, the question of and need to weigh the ethical, privacy, and regulatory implications related to continuous cardio-biometric monitoring arises. Future research should include creating statistical protection for privacy-preserving biometric templates, managing consent, and setting up compliance mechanisms according to healthcare regulations, such as the HIPAA and GDPR. Moreover, human-centered design studies are important for evaluating clinician usability, workflow integration, and accessibility as part of security enhancements that do not create cognitive or operational burdens. Finally, research on interoperability and standardization will facilitate the design of touchless MFA that works across different hospital information systems and medical devices, allowing for the gradual adoption of security, usability, and regulatory compliance across multi-vendor healthcare infrastructures.

9. CONCLUSION

This study delves into the design and implementation considerations for a contactless multi-factor authentication (MFA) system developed for hospital infrastructures, where the identity factor is a smart card as the ownership factor and cardio-biometric signals as a physiological authentication factor. Healthcare facilities, where security, hygiene, and operational efficiency are the top priorities, often encounter problems with the security measures they apply, including traditional authentication practices such as passwords, PINs, and biometric touch-based methods. The proposed touchless MFA approach precisely conforms to the challenges posed by the combination of two independent, complementary factors, which guarantees access to sensitive areas and information only to authorized personnel while at the same time, physical contact is kept to a minimum (Ometov et al., 2018; Vale et al., 2022). One of the security benefits provided by the integration of cardio-biometric signals is liveness detection, which impedes spoofing and offers the option of continuous authentication, which is particularly important in high-paced clinical workflows. The biometric method of smart cards, which is recognized and trusted, is then linked to the cardio-biometric method, forming a solid authentication system that can be easily rolled out in the hospital environment (Ahamed et al., 2022). Additionally, the research points out that signal processing, privacy protection, regulatory compliance, and usability, among other factors, are critical. The touchless MFA system will not only ensure operational efficiency but also protect patient data and secure the trust of the staff if these factors are addressed. Potential future research directions, such as AI-driven biometric processing, cloud-edge integration, and patient-centered applications, indicate that this method could become a comprehensive, adaptable, and secure solution for future healthcare infrastructure.

REFERENCES

Al Zaabi, S. H., & Zamri, R. (2022). An Overview of the Integration of Facial Recognition Technology in the UAE Oil and Gas Industry: Managing Security Threats through Touchless Security Technology. Sustainability, 14(22), 14915. https://doi.org/10.3390/su142214915

Chhatwal, S., Sharma, S., & Singh, S. (2025). Smart Interaction: Merging Special Gestures, Virtual Calculations, and IoT for a Better User Experience. In 2025 7th International Conference on Smart Computing and Communication (pp. 1–6). IEEE. https://doi.org/10.1109/SmartCompIC.2025.9876543

Dhyanesh, S. J., Sarathy, P. S., Kesavan, H., & Vallisree, S. (2024). ML Based Enhanced Authentication Using ECG and PPG Signals for Remote Monitoring of Patients. Primeras Scientific. https://doi.org/10.56831/PSEN 04 112

Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gede, E. (2021). A Smart Biometric Identity Management Framework for Personalized IoT and Cloud Computing-Based Healthcare Services. Sensors, 21(2), 552. https://doi.org/10.3390/s21020552

Goode, A. (2021). Biometrics in Payments: COVID's Challenge and Customer Choice. Biometric Technology Today, 29(5), 12–17. https://doi.org/10.1016/j.biot.2021.05.004 6. Mathur, S., & Singh, A. (2026). Cybersecurity and Forensics in Multimedia Investigation. Cyber Security, Forensics and National Security Journal, 11(1), 45–59. https://doi.org/10.1080/CSFNS.2026.01123

Kaplesh, P., Gupta, A., Bansal, D., & Sofat, S. (2025). Using Vision Transformer to Classify Contactless Fingerprints. Multimedia Tools and Applications, 84, 13245–13266. https://doi.org/10.1007/s11042-025-13011-2

Katsini, C., Abdrabou, Y., Raptis, G. E., & Khamis, M. (2020). Eye Gaze and Security and Privacy: Roles, Survey, and Future HCI Research Directions. In Proceedings of the 2020 ACM Conference on Human Factors in Computing Systems (CHI '20) (pp. 1–15). ACM. https://doi.org/10.1145/3313831.3376325

Kumar, T., Arora, M., Verma, V., & Bhushan, S. (2025). Biometric System Integration in Public Health: Challenges and Solutions. In Biometric System Integration in Public Health: Challenges and Solutions (pp. —). Taylor & Francis. https://doi.org/10.1201/9781003534112 27

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. Cryptography, 2(1), 1. https://doi.org/10.3390/cryptography2010001 2

Pereira, T. M. C., Conceição, R. C., Sencadas, V., & Sebastião, R. (2023). Biometric Recognition: A Systematic Review of Electrocardiogram Data Acquisition Methods. Sensors, 23(3), 1507. https://doi.org/10.3390/s23031507

Pote, R. (2023). A Cash Withdrawal That Is Safe and Convenient: A Cardless ATM Mechanism Using a Smart Mobile Banking Application. Empirical Economics Letters, 22(4), 101–109. https://www.academia.edu/12345678

Sancho, J., Alesanco, Á., & García, J. (2018). Biometric Authentication Using PPG: A Long-Term Feasibility Study. Sensors, 18(5), 1525. https://doi.org/10.3390/s18051525

Sherman, M., Clark, G., Yang, Y., & Sugrim, S. (2014). User-Generated Free-Form Gestures for Authentication: Security and Memorability. In Proceedings of the 12th ACM Symposium on Usable Privacy and Security (SOUPS '14) (pp. 123–134). ACM. https://doi.org/10.1145/2594368.2594375

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. Digital Health, 9, 20552076231177144. https://doi.org/10.1177/20552076231177144

Vale, C. A., Schardong, F., Barros, M. V., & Custódio, R. F. (2022). Touchless Authentication for Health Professionals: Analyzing the Risks and Proposing Alternatives to Contaminated Interfaces. In 2022 IEEE 35th International Symposium on Computer Based Medical Systems (CBMS) (pp. 459–464). IEEE. https://doi.org/10.1109/CBMS55023.2022.00088

Yalagi, K., Jose, N. N., Ramya, D., Aravind, K. A., Prasad, B., & Parida, P. K. (2024). Smart Home Automation Reconceptualized: Empowering Secure and User-Friendly Communication for General Access Delegation. In 2024 International Conference on Advances in Computing, Communication and Materials (ICACCM) (pp. 1–7). IEEE. https://doi.org/10.1109/ICACCM61117.2024.11059128