



A Literature-Based Evaluation of Cloud-Based Multi-Modal Biometric Authentication for Secure Identity Management in the Philippines

Article History:

Received: 29 March 2025

First Decision: 09 April 2025

Published: 27 June 2025

Engr. Keith B. Cauagdan¹, ORCID No. 0009-0003-0238-9347Arvin R. De La Cruz², PhD, ORCID No. 0000-0001-7325-5301¹Doctor in Engineering Management Student, Polytechnic University of the Philippines, Manila, Philippines²Chief, Graduate School Research & Extension Office, Polytechnic University of the Philippines, Manila, Philippines

Abstract

This study performs an integrative review of relevant recent scholarly articles, including peer-reviewed papers, to determine the viability of adopting cloud-based multimodal biometric authentication systems in the Philippines. Based on secondary data extracted from Scopus-indexed and ScienceDirect publications from 2020 to 2024, the study classifies findings concerning performance metrics, data protection mechanisms, and adoption determinants. The evaluation is based on a cloud-secured platform using a mix of biometric modalities such as finger, face, and iris recognition. EL_Rahman and Alluhaidan (2024) argue that multimodal systems will always outperform unimodal systems in terms of accuracy and robustness, with accuracy rates exceeding 97% and average authentication time less than 2.5 s. Moreover, users' acceptability is directly related to perceived security, usefulness, and ease of use, particularly in the e-government (Piotrowska, 2024). Security, such as homomorphic encryption and blockchain, also contributes to the protection of biometric information (Krishna, Prakasha & Sumalatha, 2025). The study emphasizes adherence to the standards set forth by existing regulations, such as the Philippine Data Privacy Act of 2012, as a fundamental ethical consideration. Offline capabilities are also emphasized as key means to address problems with connectivity, which are prevalent in rural areas (Ryu et al., 2023; DICT, 2022). Based on the Technology Acceptance Model and Information Security Theory, the study verifies the scalability and feasibility of the multi-modal biometric authentication systems in the Philippine setting. Barriers include excessive reliance on secondary sources of data and a lack of field testing. Implications for improving implementation strategies and guiding future research are provided.

Keywords: Cloud-Based Multi-Modal Biometric Authentication; Secure Identity Management; literature-based evaluation; Scopus publications; performance metrics; data protection mechanisms; adoption determinants



Copyright © 2025. The Author/s. Published by VMC Analytik's Multidisciplinary Journal News Publishing Services. A Literature-Based Evaluation of Cloud-Based Multi-Modal Biometric Authentication for Secure Identity Management in the Philippines © 2025 by Engr. Keith B. Cauagdan and Arvin R. De La Cruz is licensed under **Creative Commons Attribution (CC BY 4.0)**.

INTRODUCTION

The rising services in digitization, especially following the COVID-19 pandemic, have raised the demand for safe, accessible, and scalable identity authentication systems (Ghadge, 2024; Ryu et al., 2023). Traditional systems reliant on physical documents and static passwords are increasingly prone to breaches, inefficiencies, and a lack of inclusivity, particularly in archipelagic nations like the Philippines, where rural connectivity remains inconsistent (DICT, 2022).

Biometric technologies, including fingerprint, iris, and facial recognition, have emerged as promising solutions due to their uniqueness

and resistance to impersonation (Ametefe et al., 2025). However, challenges persist regarding data security, interoperability, and public acceptance. Hence, integrating these modalities into a cloud-based infrastructure presents an opportunity to overcome limitations in local storage, provide real-time verification, and enhance accessibility (Jasmine & Jasper, 2022). However, despite global advancements, there is limited contextual synthesis and application of these solutions in the Philippine environment. This study will therefore address this gap by reviewing and analyzing published materials and empirical findings to evaluate the viability of deploying a multi-modal biometric system grounded in current technological and policy frameworks.

Nevertheless, as expected, the implementation of such programs in the Philippine context presents challenges due to unique infrastructural, legal, and socio-cultural factors. These complexities underscore the need for localized studies or Human and Cultural Research (HCR) to develop context-specific solutions. Various biometric technologies and cloud-based systems have been anecdotally piloted and implemented in the systems operations in high-resource countries, yet these may not necessarily be immediately applicable in the Philippine context, with diverse contextual factors at play. These include disparate levels of digital literacy and poor rural connectivity, all the way to governance challenges and the need to comply with local data privacy laws. A good investment in this area is therefore the precondition for all successful realization.

This study bridges the gap by undertaking a review of literature serving as evidence to measure the fit, scale, and acceptability of a secure cloud-based multimodal biometric identity system in the Philippines and inform local understanding that can support the planning of future policy and the system. But even as technology in this regard has indeed grown, there remains a lack in parameterizing these breakthroughs to our local storyline, with unique infrastructural, legal, and cultural mores that must be taken into consideration.

Research Objectives. The study aims to analyze documented accuracy and performance benchmarks of multi-modal biometric systems. It will also seek to examine determinants of user acceptance based on previous studies applying the Technology Acceptance Model (TAM). Lastly, it aims to assess the potential of offline functionality in low-connectivity areas as reported in the literature. Based on the above objectives, the following research questions served as guides in yielding the necessary results of the study:

1. What are the documented performance benchmarks of multimodal biometric systems in terms of accuracy, speed, and reliability?
2. What security and privacy mechanisms, such as encryption and data protection frameworks, are most commonly applied in cloud-based biometric systems according to recent literature?
3. What factors influence user acceptance of biometric authentication technologies, particularly with the Technology Acceptance Model (TAM)?
4. How do current biometric systems address the challenge of low or intermittent internet connectivity, and what offline capabilities are reported to support rural and remote deployment?
5. To what extent do biometric authentication systems align with the infrastructure, policies, and socio-technical environment of countries like the Philippines, and what design considerations would ensure contextual fit?

Scope And Limitations. This study used secondary data sources from academic and peer-reviewed journals, Scopus-indexed publications, and technical reports between 2020 and 2024. Documentary analysis is employed in this study to assess the feasibility, security, and performance of cloud-based multimodal biometric authentication systems. It is not "data collection," a field test, or actual system deployment. It therefore derives its findings only based on published empirical findings and theoretical positions advanced in the recent literature.

Although these sources provide significant benchmarks and comparative analyses (EL_Rahman & Alluhaidan, 2024; Jasmine & Jasper, 2022), they may lack a comprehensive range of challenges encountered in local and practical implementations. Context-specific factors, including regional disparities in infrastructure, institutional readiness, and social and political contexts, particularly in the Philippines, also remain unmeasured in this synthesis.

As Ryu et al. (2023) note, post-hoc secondary analysis is a valuable tool to map trends and inform policy but cannot replace local pilot testing or validation by stakeholders. Although the findings of this paper are based on strong evidence, these should be cautiously generalized and also considered as benchmarks for future empirical research.

Significance of the Study. This study will synthesize and analyze validated and peer-reviewed studies to form a consolidated and credible knowledge base for policy development, strategy development for digital infrastructure, and system development. Not only does it incorporate more recent multimodal biometric authentication techniques, but it also localizes this approach in compliance with regulations and infrastructure in the Philippines. The study might also be used to argue for the modernization of national identity, such as a secure, privacy-preserving, and inclusive authentication mechanism. It is also consistent with the objectives of the Philippine Identification System Act (RA 11055) and the general local digital transformation agenda (DICT, 2022).

Theoretical Framework. The theoretical foundation of this study is the Technology Acceptance Model (TAM) and Information Security Theory – two of the most commonly used models to explain the behavioral and attitude effects toward biometric authentication technology adoption. The TAM has predictive value through variables like perceived ease of use and perceived usefulness, which are important for predicting user behavior toward new technological systems (Piotrowska, 2024). Investing alongside, Information Security Theory provides a critical perspective through which to evaluate personal privacy, integrity, and trustworthiness for both data and system issues, all of which constitute major challenges to the user acceptance of SBI systems, as introduced earlier (Kuppusamy et al., 2020; Krishna Prakasha & Sumalatha, 2025).

In the area of multi-modal biometrics connected to cloud environments, these foundations are especially relevant because a

successful deployment is not solely related to a technically efficient treatment of data, but correlated to the user's perception of security, functionality, and ease of integration with users' digital activities as well (Ryu et al., 2023; Ghadge, 2024).

With the use of these combined theoretical models, the study was able to consolidate adoption factors and risk reduction interventions into an integrated analytical structure that comprises a user-centric and a system-centric analysis.

METHODOLOGY

This study utilized documentary analysis to thoroughly investigate and combine evidence from validated academic and technical literature concerning cloud-based multimodal biometric user authentication systems. The method was based on a systematic and integrated review of peer-reviewed journal articles, technical white papers, government reports, and international standards documents, where both the most reliable and timely ones were used for analytical consideration.

The study approach was structured as an integrative review to compare and compile papers with varying techniques but analogous topics, as is typical in qualitative literature synthesis (El_Rahman & Alluhaidan, 2024; Ryu et al., 2023). The inclusion criteria were rigorously specified for maintaining methodological thoroughness, in the way that there were only empirical studies published from 2020 to 2024 in the indexed Scopus database that directly focused on biometric-cloud systems. This guarantees technical expertise, recency, and relevance of the available evidence used for the synthesis (Jasmine & Jasper, 2022; Sumalatha et al., 2024).

The researchers collected data sources from leading academic databases, including Scopus and ScienceDirect, supplemented by targeted searches using Google Scholar, to ensure inclusion of the most current and influential

publications in the fields of biometric security and cloud-based authentication technologies. A targeted and systematic search was used for literature retrieval. This comprised “multimodal biometrics,” “cloud authentication,” “biometric security,” and “Philippine digital ID,” to ensure that the study reflected both global developments as they relate to identity systems and localized relevance (Ghadge, 2024; Krishna Prakasha & Sumalatha, 2025).

After the literature corpus was gathered, a thematic analysis was performed to sort and classify the findings into the following primary analytical categories:

1. Utility metrics of a system, such as accuracy and latency;
2. Security and privacy of data, which includes security and privacy measures such as encryption and blockchains;
3. User acceptance factors based on behavioral models; and,
4. Infrastructural flexibility under low-connectivity operation (EL_Rahman & Alluhaidan, 2024; Piotrowska, 2024; Ryu et al., 2023).

As the study used only secondary data and was not conducted with human subjects, ethical issues focused on intellectual honesty: all sources were appropriately cited and credited. As there was no collection of primary data and experimentation involved, this research study complies with the academic ethical standards for documentary research and the international best practice model for the use of secondary data (Krishna, Prakasha & Sumalatha, 2025).

RESULTS AND DISCUSSION

Based on the literature, findings from the study could be broadly categorized into five main categories:

1. **System Performance.** How well the biometric system operates in terms of performance such as speed, accuracy, and

reliability, varies. A good system successfully authenticates the identity of an individual rapidly and accurately with minimal false authentications.

2. **Data Security.** That includes protecting sensitive biometric information such as fingerprints and facial data from being stolen, used improperly, or accessed by unauthorized individuals. The system is secure, making the interactions safe and reliable.
3. **User Acceptance.** How willing and how comfortable people are to use the biometric system. The easier, the more useful, and the more secure the system is for the users, the higher its acceptance and usage.
4. **Offline Capability.** This includes the fact that the system can work without the internet. It is of particular value in low connectivity or unreliable areas, such as remote or rural locations.
5. **Fit with the local infrastructure.** How closely the system fits with the technology, policies, and digital context available in a particular country or region. A good fit implies easy adoption and sustainability as per the local scenario.

For each category, authors indicate their analyses using evidence coming from peer-reviewed, Scopus-indexed publications from 2020 to 2024.

Performance. Multi-modal biometrics solutions always outperform single-modality solutions in terms of accuracy and time. The multi-modal system also has a higher false acceptance rate (FAR) and false rejection rate (FRR), because it combines multiple biometric sources such as fingerprint, face, and iris, in which the procedure of identity verification, the system's reliability is improved.

Sumalatha et al. (2024) showed that the modal fusion contributes to preventing some spoofing attacks and environmental variations. EL_Rahman & Alluhaidan (2024) carried out a

comparative analysis and reported mean recognition rates greater than 97% and mean authentication latency lower than 2.0. These numbers clearly show that multi-modal systems are highly suited for large-scale deployments, where speed and precision are of the essence.

Security. Security is the biggest challenge in the use of the biometric system in the cloud, because biometric identity is very sensitive. The current literature emphasizes the use of sophisticated cryptographic tools such as homomorphic encryption and blockchain to secure biometric data during transmission and storage (Jasmine & Jasper, 2022).

By combining these features, it is feasible to safely operate over encrypted data and maintain tamper-evident logs, hence reducing the risks of data tampering and leaking. Likewise, complying with legal and policy constraints, such as those imposed by the Philippine Data Privacy Act of 2012, RA 10173, is essential to ethical implementation and public trust. (Krishna Prakasha & Sumalatha, 2025) noted the importance of maintaining privacy in the distributed cloud, as it is becoming increasingly the more dominant computing environment.

User Acceptance. Perceived ease of use, perceived usefulness, and trust in the system to protect personal information, central constructs in the Technology Acceptance Model, all impact user acceptance of biometric systems. Piotrowska (2024) researched e-government systems and found perceived usefulness and perceived data security as determining factors for accepting biometric technology. The local implementation and implementation plans should include strategies for community empowerment and trust building that can address concerns about surveillance, misuse, and privacy breaches.

Offline Capability. Whether or not biometrics will succeed in rural or underserved rural areas depends on whether or not biometric systems can function without reliable internet. For cases like our above-the-Internet case in the

Philippines, where network access to the server is not guaranteed, or you can only access the server through your desktop, then it is essential that “offline first” becomes a first-and-foremost consideration.

EL_Rahman & Alluhaidan (2024) revealed that edge computing and secure offline authentication protocols are essential, and are finally updated to the cloud when the system is reconnected. This aspect is of critical importance for uninterrupted service provision and for the geographical spread of digital inclusion.

Contextual Fit. With heavy smartphone penetration, a mobile-first design makes sense for the Philippine setting. Building for mobile first with desktop as a backfill is a forward-thinking model that accounts for the long-term trend of more and more people doing things on smart devices. This is even more relevant in archipelagic and emerging markets where the access point to the digital world is, in fact, mobile. A mobile-first approach can greatly improve scalability and, as a result, inclusiveness. This innovation makes it easier to create new connections between and across digital divides and improves interaction within the ecosystem of national identification systems.

In addition, the incorporation of privacy-preserving frameworks ensures that the deployment of the system is indeed feasible for national identity projects with a lower risk in terms of legal and ethical concerns. Ryu et al. (2023) pointed out that cloud-based biometric systems can be effectively and simply extended to operate in localized environments, provided that adaptability and governance are core enough to their design and development.

Conclusion. The integrative review affirms that the cloud-based Multi-Modal Biometrics System is acceptable for secure and inclusive identification in the Philippines. Where appropriately domesticated to local legal frameworks, national connectivity infrastructure, local cultural norms, and overall contextual fit, these systems offer one pathway

to scale, helping to influence trust, access, and efficiency related to the management of national digital identity. They are valuable not only for being technically feasible, but for their ability to widen access divides and further the country's overarching digital transformation efforts.

Empirical data indicate that such systems tend to achieve high-performing results as measured in terms of accuracy and responsiveness (El_Rahman & Alluhaidan, 2024; Sumalatha et al., 2024), as well as security improvements with advanced cryptographic methods such as homomorphic encryption and blockchain (Krishna Prakasha & Sumalatha, 2025).

User acceptance is determined by the perception of security, usefulness, and ease of use, which can be reflected in the Technology Acceptance Model (Piotrowska, 2024). Importantly, the feasibility of the system is enhanced by its potential to function offline, which is a necessary feature for the deployment of the system in low-resource rural areas with intermittent network connections (El_Rahman & Alluhaidan, 2024; Ryu et al., 2023).

Equally important is that the mobile-first designs are scalable, easily adaptable to other institutional set-ups, compatible with the national data governance policies, including (RA 10173) Data Privacy Act of 2012 and (RA 11055) Philippine Identification System Act, and indicative of the readiness of the system for local implementation.

Recommendations. In light of this converging evidence and the need for the Filipino virtual world, the following recommendations have been proposed to be implemented:

1. Implement biometric solutions that are mobile-enabled and capable of working without internet. By taking performance without constant internet connection to people, along with its inclusivity in identity claims (El_Rahman & Alluhaidan, 2024), we'll open up access to these systems to rural and underserved populations.

2. Strong encryption, which is also to be followed according to whichever local laws are currently in place regarding data protection. A clause or law similar to RA 10173 and RA 11055 would facilitate the formation and execution of biometric systems at the same time, boosting confidence and trust of users (Krishna Prakasha & Sumalatha, 2025).
3. Engage in civic education and enlightenment sensitization. Communication approaches are required to enhance the clarity on what is known about the technology, upper reduce predictable resistance, and to foster a responsible use of the technology by the citizens (Piotrowska, 2024).
4. The on-site pilot trials and the need-based assessment at each site. Pilot-indicators can collect context cognition, real operation performance, and feedback strategy adjusted according to stakeholder's perceptions (Ryu et al., 2023).

Cloud-based multimodal biometric systems are a secure, scalable, and contextually relevant solution for the Philippines. But making it work will take more than technical readiness; it will require institutional buy-in, legal protections, and broad public uptake.

Future Research Directions. While the present study gives an in-depth literature overview on the subject of cloud-based multi-modal biometric authentication systems, some issues still need to be subjected to empirical scrutiny. Further research is therefore recommended, with an emphasis on conducting targeted studies to inform policy and system development in the following areas:

1. *Comparative analysis that covers all of ASEAN.* Future studies may consider the implementation of biometric ID systems in the 10 ASEAN members to compare and contrast policy framework, infrastructure preparedness, user acceptance, and system scalability. Such regional studies may not only unearth best practices for successful transformation to the digital age, but also

struggles that are widely shared, especially in culturally and economically diverse settings that aspire to similar digital development goals.

2. **General Cost and Benefit and Return on Investment (ROI) Analysis.** Few detailed economic evaluations of biometric identity system deployments exist. Assessment of the long-term financial sustainability, cost-effectiveness, and operational benefits of national ID programs could provide powerful legitimization for large investments. Such assessments should encompass objective as well as subjective benefits, such as the effectiveness of the service and the confidence of the public.
3. **User acceptance long-term study.** Most studies in the literature are single measurements. It is necessary to keep longitudinal data to more clearly understand how distrust in such systems, security concerns, and usage develop in the long run following deployment. This is particularly relevant in real-life situations, in which resistance to initially unfamiliar food may be compromised as familiarity increases.
4. **Expectations of National Digital ID Systems.** When countries such as the Philippines are beginning to consider national digital ID programmers, further discussion is required around how biometric systems can be effectively integrated into broader e-governance services. Researchers should inquire about interoperability issues, data harmonization, and cross-agency use of biometric credentials to guarantee that system design is also aligned with the country's national digital transformation path and the applicable legislations like RA 11055.

By addressing these challenges, future work can be informed by evidence-based, more persistent approaches to the deployment of secure, inclusive identity authentication systems in local and regional settings.

Ethical and Legal Considerations. This study utilized secondary data obtained from peer-reviewed journal articles, government reports, and technical publications from 2020 to 2024. Because direct patient recruitment and primary data collection were not performed, this study met the criteria for Institutional Review Board (IRB) exemption. As such, information on the processes of informed consent, data retention and erasure, cross-border transfer of data, and notification of breaches, processes that are commonly included in empirical research with human subjects, was neither sought nor relevant in this review.

Academic integrity and intellectual honesty were observed all along. All referenced contributions were sufficiently and accurately referred to, and no data were manipulated or falsified from previous reports. The study also adhered to best scholarly practice by considering the entirety of the evidence impartially and without introducing any bias or giving undue emphasis to particular findings.

In terms of legal and regulatory issues, we acknowledge that any prospective realization of a cloud-based biometric ID authentication system in our country should conform to the appropriate national laws. This includes Republic Act No. 10173, also known as the Data Privacy Act of 2012, and Republic Act No. 11055, otherwise known as the Philippine Identification System Act, which have outlined the parameters on the administrative processing and protection of personal and biometric information.

For any new system, there are also requirements to assess the need for registering the processing with the National Privacy Commission (NPC), performing responsibilities related to risk and data protection impact assessment, and observing incident reporting. This study, although not involved in the primary data processing itself, recognizes the ethical and sociopolitical perspectives that must underpin the use of biometric technologies, particularly in the context of public sector usage. These are principles such as respect for the rights of the data subject, free and informed

consent, transparency, data minimization, and accountability.

Equally importantly, future systems need to be compliant not just with the legal obligations, but with individual rights to data ownership, portability, the right to be forgotten, and algorithmic compliance, each of them necessary to preserve a set of ethical constraints that society will require for biometric technology to be trusted as it becomes increasingly omnipresent.

Although this work does not provide empirical evidence, it has some implications for the ethical debate, as it points out mandatory privacy by design, legally compliant system development, and responsible innovation in the use and management of biometric-based identity assurance.

As technology advances, embracing international standards on human rights will become increasingly important to protect individual autonomy and prevent abusive or discriminatory use of biometric systems.

REFERENCES

- Ametefe, D. S., Sarnin, S. S., Ali, D. M., Ametefe, G. D., John, D., & Hussin, N. (2025). Advancements and challenges in fingerprint presentation attack detection: a systematic literature review. *Neural Computing & Applications*, 37(4), 1797–1819. <https://doi.org/10.1007/s00521-024-10423-8>
- EL_Rahman, S. A., & Alluhaidan, A. S. (2024). Enhanced multimodal biometric recognition systems based on deep learning and traditional methods in smart environments. *PLoS ONE*, 19(2), e0291084. <https://doi.org/10.1371/journal.pone.0291084>
- Department of Information and Communications Technology [DICT]. (2022). *National ICT Household Survey 2019*. https://ictstatistics.dict.gov.ph/wp-content/uploads/2022/06/National-NICTHS-Results_Updated-June-2022.pdf.
- Ghadge, N. (2024). Challenges with securing digital identity. *International Journal on Cybernetics & Informatics*, 13(4), 01–08. <https://doi.org/10.5121/ijci.2024.130401>
- Jasmine, R. M., & Jasper, J. (2022). A privacy preserving based multi-biometric system for secure identification in cloud environment. *Neural Processing Letters*, 54(1), 303–325. <https://doi.org/10.1007/s11063-021-10630-7>
- Krishna, C., Prakasha, K., & Sumalatha, U. (2025). Privacy-preserving techniques in biometric systems: Approaches and challenges. *IEEE Access: Practical Innovations, Open Solutions*, 13, 32584–32616. <https://doi.org/10.1109/access.2025.3541649>
- Kuppusamy, P., Samy, G. N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B., & Perumal, S. (2020). Systematic Literature Review of Information Security Compliance Behaviour Theories. *Journal of Physics Conference Series*, 1551(1), 012005. <https://doi.org/10.1088/1742-6596/1551/1/012005>
- Piotrowska, A. I. (2024). Determinants of consumer adoption of biometric technologies in mobile financial applications. *Economics and Business Review*, 10(1). <https://doi.org/10.18559/eb.2024.1.1019>
- Ryu, R., Yeom, S., Herbert, D., & Dermoudy, J. (2023). The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. *ICT Express*, 9(6), 1183–1197. <https://doi.org/10.1016/j.icte.2023.04.003>

Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. *IEEE Access: Practical Innovations, Open Solutions*, 12, 64300–64334.
<https://doi.org/10.1109/access.2024.3395417>

Republic Act No. 10173. (2012). *Data Privacy Act of 2012. Official Gazette of the Republic of the Philippines*.
<https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/>

Republic Act No. 11055. (2018). *Philippine Identification System Act. Official Gazette of the Republic of the Philippines*.
<https://www.officialgazette.gov.ph/2018/08/06/republic-act-no-11055/>