# BIOMETRIC CLOUD-BASED AUTHENTICATION SYSTEM USING BLOCKCHAIN TECHNOLOGY AND RASPBERRY PI AT THE UNIVERSITY OF PERPETUAL HELP SYSTEM LAGUNA – ISABELA CAMPUS

**Alforo, Jemel**
**Corpuz, Ryan**
**Fernandez, Czylon**
**Tabago, Maricel**
**Fortuna, Rochelle**
**Garduque, Rovelinda**
University of Perpetual Help System Laguna-Isabela Campus
Cauayan City, Isabela

***Abstract*— The University of Perpetual Help System Laguna – Isabela Campus currently utilizes a manual attendance logging system, which not only consumes excessive paper resources but also contributes to inefficiencies in data entry and storage. To address these challenges, this project developed a Biometric Cloud-Based Authentication System that integrates Blockchain Technology and Raspberry Pi to enhance security, transparency, and authentication processes. Designed specifically for authorized personnel, the system captures fingerprint data, encrypts it using blockchain mechanisms, and securely stores it in a cloud database for efficient management and retrieval. By eliminating traditional paper-based methods, the system significantly reduces security risks associated with conventional authentication practices. The successful implementation of this project offers a model for educational institutions and other organizations aiming to strengthen security measures while streamlining operational workflows. Overall, this innovation advances biometric-based authentication by leveraging cutting-edge technologies to ensure data integrity, privacy, and accessibility.**

**Keywords—** *Biometric Authentication, Blockchain, Cloud-Based System, Raspberry Pi, Secure Access*

## I. INTRODUCTION

Biometric authentication systems have become critical in enhancing the security of identity verification processes. These systems leverage unique biological traits—such as fingerprints, facial recognition, and voice patterns—to provide reliable access control (Saleh Alwahaishi & Jaroslav Zdrálek, 2021). Meanwhile, the growing threat of cyberattacks underscores the need for more robust authentication mechanisms, as cybercriminals continually develop sophisticated techniques to breach traditional security systems. In response to this, blockchain technology has emerged as a secure and decentralized solution, ensuring that data stored within its system is tamper-proof, transparent, and highly resistant to unauthorized manipulation (Carmen B. et al., 2021; Durga R. et al., 2022).

The importance of integrating biometric authentication with blockchain has been recognized in various sectors, including finance, healthcare, and smart city initiatives. As noted by Gorkhali et al. (2020), blockchain's distributed ledger structure provides a trustworthy environment for managing sensitive personal data. Furthermore, studies by Amara Devendra Dinesh et al. (2021) emphasized that combining blockchain and biometrics offers a powerful defense against identity theft, ensuring that biometric templates remain immutable and secure. However, despite these promising advancements, current systems often lack scalability, portability, and real-time monitoring capabilities, especially within educational institutions where manual recordkeeping remains prevalent.

Recognizing these challenges firsthand, the researchers were motivated to pursue this project after observing the traditional attendance logging system at the University of Perpetual Help System Laguna – Isabela Campus. This was envisioned where the university faced operational setbacks during accreditation due to incomplete or lost manual

attendance records. This highlighted the urgent need for a system that is not only secure but also efficient, transparent, and paperless. Consequently, the researchers designed the Biometric Cloud-Based Authentication System Using Blockchain Technology and Raspberry Pi, aimed at resolving the inherent inefficiencies of manual systems while addressing modern security requirements.

The purpose of this study is to develop a cloud-based biometric authentication system that securely captures and stores fingerprint data, integrating blockchain technology to ensure transparency, data integrity, and security. The system also seeks to enhance usability, efficiency, reliability, and maintainability, offering a seamless user experience through a mobile application interface powered by Raspberry Pi.

This study significantly contributes to the community by promoting a secure, eco-friendly, and technologically advanced authentication system that can be adapted by other institutions. It offers a model for sustainable digital transformation, streamlining operational workflows while upholding high security standards. Furthermore, by reducing the reliance on paper and manual procedures, the system supports the university's initiatives toward digitalization and environmental stewardship.

While previous studies demonstrated either biometric innovations or blockchain integration separately, few have successfully combined these technologies into a unified, cloud-based, scalable authentication system suitable for institutional environments. Moreover, gaps such as the absence of mobile monitoring applications and lack of flexible deployment have limited the full realization of these technologies in educational settings. Therefore, this project addresses these gaps by merging biometrics, blockchain, cloud storage, and mobile application functionalities into one comprehensive solution.

To address these gaps, the proposed solution involves the development of a Biometric Cloud-Based Authentication System utilizing a Raspberry Pi microcontroller integrated with fingerprint sensors and a blockchain-secured cloud database. The system captures users' biometric data, encrypts it using blockchain principles, and securely transmits and stores it in a cloud environment. Authorized personnel can access and monitor authentication logs in real time through a mobile application. This solution ensures data immutability, enhances operational efficiency, reduces resource consumption, and fortifies the university's data security posture, serving as a sustainable model for digital identity management across academic institutions.

## II. METHODS

The study adopted a descriptive-developmental research design. The descriptive aspect focused on gathering information regarding the existing manual attendance system of the university, while the developmental aspect emphasized the design and creation of the proposed biometric authentication system.

The system was developed using the Iterative Development Model, which allowed for continuous refinement of functionalities and design based on feedback from each cycle. Requirement analysis was first conducted through surveys and informal interviews with staff to identify limitations of the manual system and determine priority features such as secure data storage, real-time monitoring, and user-friendly interfaces. These requirements informed the control system design, which included data flow management from biometric input to encryption and cloud storage, with blockchain mechanisms integrated to enhance security. Authentication tokens were also incorporated to regulate system access.

Software modeling and simulation were conducted using Python and Flutter/Dart to test the initial design. Identified issues were immediately corrected, ensuring an agile yet reliable development process. The hardware prototype was then assembled using Raspberry Pi 4B, a fingerprint sensor (AS608), a temperature sensor (MLX90614), and a touchscreen display, with the Raspberry Pi serving as the central processing unit to capture, encrypt, and transmit biometric data to the cloud. Functional testing followed, focusing on fingerprint registration and authentication, as well as secure data transmission to blockchain and cloud infrastructures. Identified errors were corrected and retested until reliable performance was achieved.

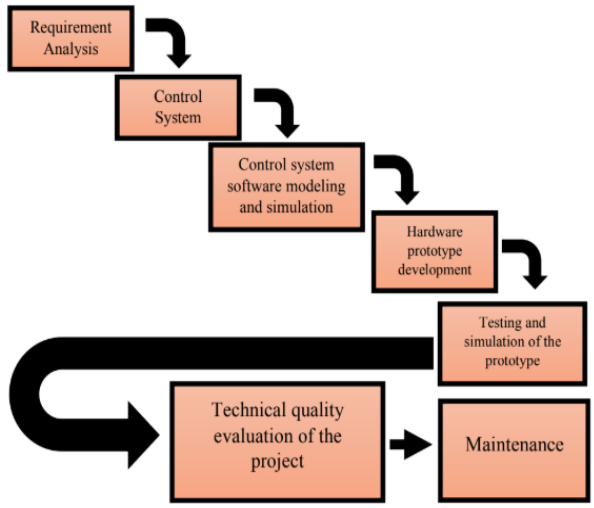
To further ensure technical soundness, the project underwent evaluation by experts who assessed usability, efficiency, security, reliability, and maintainability. The results confirmed that the system aligned with both academic and industry standards. In preparation for long-term sustainability, maintenance procedures were also outlined, including periodic software updates, hardware inspections, and cloud-blockchain monitoring. Documentation was prepared to guide future users and developers in system upkeep.

The participants of the study consisted of 66 non-teaching employees of the University of Perpetual Help System Laguna – Isabela Campus, selected through stratified sampling. Data were gathered using structured survey questionnaires developed by the researchers. These instruments were designed to evaluate the limitations of the current manual attendance system and the effectiveness of the developed biometric system. Content validity was established through review by a research adviser, instructor, and statistician, while internal consistency was confirmed through a pilot test, with Cronbach's Alpha applied to verify reliability.

For the data-gathering procedure, approval was secured from the school director, and letters were submitted along with the pre-survey questionnaires detailing the scope and purpose of the study. After securing permission, the

questionnaires were distributed and retrieved from respondents. The data collected were organized and analyzed in accordance with the research objectives, specifically focusing on the evaluation criteria of usability, efficiency, reliability, security, and maintainability. Weighted mean was used as the primary statistical tool to compute the overall evaluation of the biometric authentication system.

Ethical standards were carefully observed throughout the study. Informed consent was obtained from all participants, and their anonymity and confidentiality were strictly maintained. Respondents were informed of their right to decline or withdraw participation at any point without penalty. The researchers also upheld the principles of honesty, integrity, and transparency in data collection, analysis, and reporting, ensuring that results were presented objectively and without bias.




## III. RESULTS AND DISCUSSION

**Table 1. Mean Distribution of the Traditional Biometrics**

| Statement | Mean | Interpretation |
|---|---|---|
| Traditional biometric systems are prone to security breaches or unauthorized access due to identity theft and spoofing. | 4.39 | Strongly Agree |
| Lack the flexibility to adapt to changing security requirements, leaving them vulnerable to emerging threats and evolving attack methods. | 4.34 | Strongly Agree |
| Lack of interoperability, making it challenging to integrate them with other systems and technologies. | 4.18 | Agree |
| Often struggle to maintain accuracy and reliability over extended periods, leading to potential authentication failures. | 4.30 | Strongly Agree |
| Raise concerns about data storage and management, particularly regarding the long-term retention and secure disposal of biometric information. | 4.45 | Strongly Agree |
| Performance degradation, especially in high-traffic scenarios or under adverse environmental conditions. | 4.31 | Strongly Agree |
| Struggle to accurately authenticate individuals with certain physical or medical conditions, such as injuries or disabilities. | 4.21 | Strongly Agree |
| Traditional biometric systems can be expensive to implement and maintain, particularly when deployed across large organizations. | 4.28 | Strongly Agree |
| Often lack a robust audit trail and transparency in user authentication. | 4.39 | Strongly Agree |
| Have limitations in terms of scalability and adaptability to different applications. | 4.40 | Strongly Agree |
| **GRAND MEAN** | **4.33** | **Strongly Agree** |

Table 1 shows the widespread dissatisfaction with traditional biometric systems, particularly in areas like data storage, security, interoperability, and adaptability to emerging threats. The highest concern (Mean = 4.45) was related to the secure storage and disposal of biometric information. These findings reflect similar concerns raised by Zyskind, Nathan, and Pentland (2015), who argued that centralized biometric systems are vulnerable to data tampering and privacy violations. Additionally, Amara Devendra Dinesh et al. (2021) emphasized that traditional systems often fall short in addressing identity spoofing and storage transparency—highlighting the need for blockchain-enhanced solutions like the one developed in this study.

**Table 2.1 Mean Distribution in Terms of Usability**

| Statement | Mean | Interpretation |
|---|---|---|
| The biometric cloud-based authentication system is easy to use and has simple interfaces to make it user-friendly. | 4.5 | Strongly Agree |
| It lets users choose how they want to prove their identity, making it flexible to register an account. | 4.45 | Strongly Agree |
| A user will find it easy to learn how to use the system, it is designed to be simple. | 4.45 | Strongly Agree |

| | | |
|---|---|---|
| Users will get clear guidelines on how to use the system. | 4.62 | Strongly Agree |
| The system is designed to be accessible for people with different levels of experience and abilities. | 4.63 | Strongly Agree |
| **GRAND MEAN** | **4.53** | **Strongly Agree** |

Table 2.1 shows the evaluation of the Biometric Cloud-based Authentication System in terms of Usability. With a grand mean of 4.53, respondents strongly agreed that the biometric cloud-based system was user-friendly, easy to navigate, and accessible for users with varying levels of experience. This aligns with the findings of Ashraf and Ali (2020), who found that biometric systems designed with clear interfaces and intuitive processes lead to higher user acceptance and efficiency. The integration of a mobile app interface using Flutter/Dart also enhanced the system's accessibility, supporting the work of Alzubaidi and Kalutarage (2021), who emphasized the importance of usability in educational technology tools for widespread adoption.

**Table 2.2 Mean Distribution in Terms of Efficiency**

| **Statement** | **Mean** | **Interpretation** |
|---|---|---|
| The system works quickly, so people don't have to wait long to confirm their identity. | 4.57 | Strongly Agree |
| The system doesn't use too much power or resources. | 4.71 | Strongly Agree |
| The system is compact and doesn't take up much space wherever you place it. | 4.65 | Strongly Agree |
| It allows the user to export data in a ready Excel document format. | 4.52 | Strongly Agree |
| Automatically updates data procedures minimize downtime and ensure continuous performance. | 4.56 | Strongly Agree |
| **GRAND MEAN** | **4.60** | **Strongly Agree** |

Table 2.2 shows the evaluation of the Biometric Cloud-based Authentication System in terms of Efficiency. The system's efficiency scored a high mean of 4.60, showing that users appreciated its speed, low power/resource consumption, compactness, and seamless data export features. This finding is supported by Sathishkumar and Sumathi (2018), who implemented a Raspberry Pi–based attendance monitoring system and noted its resource efficiency, portability, and practicality for institutions. Moreover, the automatic updating feature, as highlighted in the system, contributes to reduced administrative load and continuous system performance—qualities that are critical in educational environments.

**Table 2.3 Mean Distribution in Terms of Security**

| **Statement** | **Mean** | **Interpretation** |
|---|---|---|
| The system makes sure that people's information is kept safe using different layers of protection. | 4.56 | Strongly Agree |
| The system keeps a record of everyone who uses it and makes sure that no one can tamper the authentication process. | 4.64 | Strongly Agree |
| The system enforces strict access controls and authentication protocols to prevent unauthorized usage and potential breaches. | 4.65 | Strongly Agree |
| The system prevents data tampering by using blockchain technology to verify the authentication records in the cloud. | 4.6 | Strongly Agree |
| The system undergoes testing and validation to uphold accuracy and precision in biometric recognition and authentication. | 4.62 | Strongly Agree |
| **GRAND MEAN** | **4.61** | **Strongly Agree** |

Table 2.3 shows the evaluation of the Biometric Cloud-based Authentication System in terms of Security. Security has a strong mean of 4.61, underscoring user confidence in the system's multi-layered protection, blockchain-based data integrity, and secure authentication processes. These findings align with Yaga et al. (2019), who documented how blockchain's decentralized ledger ensures tamper-proof authentication logs, making it ideal for identity systems. Additionally, Carmen B. et al. (2021) noted that blockchain technologies add transparency and auditability, which directly addresses the shortcomings observed in traditional biometric systems from the pre-survey results.

**Table 2.4 Mean Distribution in Terms of Reliability**

| **Statement** | **Mean** | **Interpretation** |
|---|---|---|
| The system is designed to work consistently, so people can rely on it whenever they need to. | 4.51 | Strongly Agree |
| The system has the ability to automatically resolve issues and restore functionality if something goes wrong. | 4.42 | Strongly Agree |

| | | |
|---|---|---|
| If a part of the system fails, there are backup measures in place to ensure uninterrupted operation. | 4.60 | Strongly Agree |
| Extensive testing has been conducted to ensure its accuracy and dependability. | 4.59 | Strongly Agree |
| It seamlessly integrates with other systems and processes. | 4.63 | Strongly Agree |
| **GRAND MEAN** | **4.55** | **Strongly Agree** |

**Table 2.4** shows the evaluation of the Biometric Cloud-based Authentication System in terms of Reliability. With a grand mean of 4.55, respondents agreed that the system operates consistently, has built-in recovery features, includes backups, and integrates well with other institutional systems. This matches the conclusions drawn by Alzubaidi and Kalutarage (2021), who emphasized the need for resilient authentication systems in academic institutions to support uninterrupted operations. The presence of robust fallback and error-handling mechanisms strengthens users' trust and system sustainability.

**Table 2.5 Mean Distribution in Terms of Maintainability**

| **Statement** | **Mean** | **Interpretation** |
|---|---|---|
| The system architecture facilitates modular upgrades and expansions, easy to add new things to the system's future enhancements and features. | 4.60 | Strongly Agree |
| Users have access to comprehensive resources for maintaining the system's functionality. | 4.62 | Strongly Agree |
| The system conducts self-assessments support to the server to ensure optimal performance. | 4.48 | Strongly Agree |
| Regular checks and maintenance by the developers ensure that the system consistently performs as intended. | 4.51 | Strongly Agree |
| When the system reaches the end of its useful life, its decommissioning will adhere to environmental safety standards and regulations. | 4.54 | Strongly Agree |
| **GRAND MEAN** | **4.55** | **Strongly Agree** |

**Table 2.5** shows the evaluation of the Biometric Cloud-based Authentication System in terms of maintainability. Maintainability was rated positively with a mean of 4.55. Users appreciated the modular architecture, support resources, self-assessment tools, and environmentally responsible decommissioning plans. These findings are echoed by Sathishkumar and Sumathi (2018), who emphasized that systems built on flexible platforms like Raspberry Pi allow for easy updates and long-term maintainability. Moreover, the modular nature of the system positions it well for future expansions and integration with emerging technologies such as AI-based anomaly detection and multi-factor authentication.

## V.CONCLUSION AND RECOMMENDATIONS

The study successfully developed and evaluated a Biometric Cloud-Based Authentication System using Blockchain Technology and Raspberry Pi to address the inefficiencies of the university's manual attendance process. The system received strong positive feedback for its usability, efficiency, security, reliability, and maintainability. It offers a practical and sustainable solution that enhances data accuracy, reduces administrative workload, and supports the institution's move toward digital transformation.

## REFERENCES

Alzubaidi, M. A., & Kalutarage, H. (2021). *Enhancing educational systems through biometric authentication*. *Education and Information Technologies*, 26(1), 923–939. https://doi.org/10.1007/s10639-020-10294-3

Almeida, P., Garcia, A., & Silva, M. (2023). *Energy-efficient systems for biometric authentication using edge computing: A review*. *Journal of Computational Engineering*, *12*(3), 112–125. https://doi.org/10.1016/j.jce.2023.01.001

Amara Devendra Dinesh, R., Vasanth, K., & Saranya, M. (2021). *Securing biometric data using blockchain technology*. *International Journal of Computer Applications*, 183(11), 1–6.

Ashraf, M. W., & Ali, S. (2020). *User acceptance of biometric authentication in online transactions: An empirical study*. *International Journal of Computer Science and Information Security*, 18(1), 24–30.

Calo, A.-M. V., Barbosa, J. B., & Llevado, J. C. (2021). In-classroom faculty attendance monitoring system based on ultra high frequency (UHF) RFID with captured image cross-verification mechanism. *Indian Journal of Science and Technology*, *14*(45), 3335–3343. https://doi.org/10.17485/IJST/v14i45.1782

Carmen, B., Martínez, A., & López, C. (2021). *Blockchain-based authentication systems for secure identity verification: A review*. *Sensors*, 21(10), 3401. https://doi.org/10.3390/s21103401

Cuya, K. C., & Palaoag, T. D. (2024). Blockchain in higher education: Advancing security, verification, and trust in academic credentials. *Nanotechnology Perceptions, 20*(S3), 373–386.

Durga, R., Ramu, P., & Suresh, K. (2022). *Securing biometric data using blockchain technology: A comprehensive review*. Materials Today: Proceedings, 56, 2298–2303. https://doi.org/10.1016/j.matpr.2022.03.605

Gorkhali, A., Li, J., & Shrestha, A. (2020). *Secure and decentralized biometric authentication using blockchain*. In Proceedings of the 2020 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1–6). IEEE. https://doi.org/10.1109/ICCE46568.2020.9043082

Nueva, C. H., Tapic, F. M. J., Pineda, I. T., Melendrez, J. K. T., Jimena, P. C., & Alquiza, R. J. (2024). RFID-based student attendance monitoring system with SMS notification using Arduino for Bestlink College of the Philippines. *Ascendens Asia Singapore – Bestlink College of the Philippines Journal of Multidisciplinary Research*, *3*(1A). Retrieved from

https://ojs.aaresearchindex.com/index.php/aasgbcpjmra/article/view/12810

Philippine Institute for Development Studies. (2021, November 5). *Blockchain and government efficiency* [Policy note]. Retrieved from https://www.pids.gov.ph/details/blockchain-and-government-efficiency

Saleh Alwahaishi, & Jaroslav Zdrálek. (2021). *Biometric authentication systems: Developments, challenges, and trends*. Information Security Journal: A Global Perspective, 30(4), 186–195. https://doi.org/10.1080/19393555.2021.1933607

Sathishkumar, V. E., & Sumathi, R. (2018). *Smart attendance monitoring system using Raspberry Pi*. *International Journal of Innovative Research in Computer and Communication Engineering*, 6(3), 232–237.

Shah, A., & Kumar, V. (2022). *Biometric-based authentication systems for academic environments: A review and future trends*. *Journal of Higher Education Technology*, *11*(3), 215–229. https://doi.org/10.1016/j.jhet.2022.05.008

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain technology overview* (NIST IR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

Zhang, X., Wang, Y., & Zhao, L. (2020). *Cross-platform applications for university security systems: A case study using biometric solutions*. *Journal of Mobile Technology and Security*, *5*(2), 101–113. https://doi.org/10.1016/j.jmts.2020.02.007

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security and Privacy Workshops (SPW)*, 180–184. https://doi.org/10.1109/SPW.2015.27