RESEARCH ARTICLE

DOI: 10.34256/ijcci2517

International Journal of Computer Communication and Informatics

Automated System to Preventing Social Security Fund Misuse by Identifying Deceased Beneficiaries

N. Uma Maheswari [a,*], K. Nagaraj [a], S. Nitheesh [a], K. Mirthick [a], P. Nagapugalarasan [a]

[a] PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India

* Corresponding Author: nagarajkannan2003@gmail.com

Received: 19-02-2025, Revised: 14-04-2025, Accepted: 22-04-2025, Published: 06-05-2025

Abstract: Ensuring safe and convenient access to essential services, including pension retrieval, is crucial in the current digital era. Passwords and PINs are examples of traditional authentication systems that frequently expose people to fraud and identity theft. In order to replace these traditional methods with biometric verification (such as fingerprint and facial recognition), this project suggests a Web Biometric Credentialing System for pension retrieval. The system incorporates Auth0 for secure identity and management of sessions and WebAuthn API for biometric authentication. This method greatly enhances security and user experience by enabling pensioners to verify their identity using biometric information. The technology makes sure that only authorized people can access sensitive financial data and, after successful verification, enables pensioners to safely retrieve their pension amounts. By lowering fraud, eliminating unwanted access, and streamlining the authentication procedure, the suggested solution improves security.

Keywords: Game Theory, Incentives, Security Economics, and Retail Payment Security, MFA, JWT, Auth0 SDK.

1. Introduction

The goal of this project is to use web technologies to create a safe and effective biometric authentication system for pension retrieval. The technology enables retired people to safely access and receive their pension payments by authenticating themselves using biometric information (such as a fingerprint or facial recognition). Identity management is handled by Auth0, and the system's backend, Express.js, offers a smooth authentication process. By substituting biometric authentication for the conventional password-based login, this system improves security by guaranteeing that only authorized users can access their pension data. Identity verification techniques that are safe, effective, and easy to use are more important than ever, especially for vital services like pension retrieval. Pension funds are a major source of financial stability for retirees in many nations. Passwords, PINs, and physical identification

documents are examples of traditional means of obtaining pension information that are frequently slow, laborious, and vulnerable to fraud or identity theft. The need to give pensioners a more safe, efficient, and easily accessible way to access their pension data has grown as a result of the digitization of services. The limits of conventional identification techniques have been addressed by biometric authentication, which makes use of distinctive physical characteristics like fingerprints, facial recognition, or retinal scans. This technology not only increases security by lowering the possibility of fraud, but it also improves user experience by providing a quicker and easier method of identification verification.

2. Literature Review

We examined the effectiveness of several demographic factors in creating connections between patient registry records from two hospital registries and the Social Security Death Master File as part of creating a record linkage algorithm using de-identified patient data [1]. To create a linkage gold-standard, we examined 6,000 record-pair samples from each registry. With Social Security Number as the sole linkage variable, significant linkage error rates of 4.7% and 9.2% were obtained. Social Security Number, phonetically compressed first name, birth month, and gender were the most effective single variable combinations for identifying connections. Eighty-seven and eight-eight percent of the links were judged to be genuine. By combining the social security number, gender, name, and birthdate information, we were able to reach 90% to 92% sensitivities while keeping 100% specificity. A more generalized de- identified linkage algorithm is based on this precise approach of connecting patient information to death data.

There is still a lack of research on the idea that biometric technologies can improve service delivery and secure private data. In order to fill this knowledge vacuum, we use the information security model of confidentiality-integrity-availability as an analytical lens and a qualitative interpretative study approach to examine the case of a public-sector social security and pension organization in Ghana [2]. The results of the study show that information availability, confidentiality, and integrity can be safeguarded by incorporating and utilizing biometric identification and authentication into the provision of social security and pension services. The results also demonstrate that the use of a biometric system for the security of social security and pension data can help to decrease service response times and susceptibility to fraudulent benefit payment manipulation. The study has policy, practice, and research implications. The paper makes it possible to conduct research on biometric systems from the standpoints of information security and service enhancement. The study highlights the significance of matching the deployment and use of biometric technologies with domain application needs for practice and policy.

The primary goals of this research project, Design and Implementation of Tax Payment System utilizing Fingerprint Biometrics and Bank Verification Number, are to enhance voluntary compliance, reduce tax evasion, and streamline tax administration [3]. The goal of the project was to create a system that could record the fingerprints and bank verification numbers of

employers, employees, entrepreneurs, and craftspeople and use them to track and validate their tax-related activities whenever they choose. This work is motivated by the challenges tax authorities face in persuading individual taxpayers to pay their taxes through the sharing of demand notices, closing of business outlets, etc.; the failure and delay of many private enterprises in filing employee returns; the diversion and leakage of generated funds by dishonest tax and bank officials; the forgery of tax certificates; and the widespread tax evasion in our society today. Object- oriented hypermedia design methodology (OOHDM) is the approach used. One of the earliest approaches to propose the division of issues defining its several models— requirements, conceptual, navigation, abstract interface, and implementation—is OOHDM. To construct the tax payment system, JavaScript, PHP, HTML, and MySQL were utilized. The system offers interfaces that allow tax authorities to register, amend, and confirm the tax payment compliance status of individual taxpayers as well as employees of businesses. The system's outcomes include giving tax authorities and other government agencies a way to confirm taxable individuals, allowing taxpayers to pay and view their tax history from the convenience of their homes, and enabling the bank plug- in to track and send convincing text messages to any tax evaders or defaulters during bank transactions.

The growth potential of carefully thought-out cash transfer schemes has attracted a lot of attention in recent years [4]. One specific use is when resource-rich nations employ transfers to divide rents among their citizens, as Iran has lately done. According to a growing body of research, these initiatives typically have a positive development impact and can help impoverished people or households overcome obstacles to economic activity, which in turn can lead to an additional gain in income. In the institutional conditions that are prevalent in many developing nations, this study examines the use of biometric technology to support transfer programs and how new technology is creating opportunities for successful transfer programs that were previously merely theoretical. Banking, voting, healthcare, and general identifying systems are just a few of the many other development projects that biometric identification systems can help with once they are put into place. Similar to how the cellphone revolution revolutionized communications, the study examines some of the initiatives that use these technologies and how they are helping poor countries overtake rich ones in the domain of identity.

Nowadays, personal identification is a necessary precondition for progress in the contemporary society [5]. The provision of appropriate identification cards enhances citizens' access to public and private services and aids governments in better understanding and serving their constituents. States are using biometrics, most frequently fingerprints, to integrate more robust (unique, secure, and accurate) identity systems in an attempt to make them as accurate and unique as possible. From a large-scale government standpoint, the systems appear to be functional; however, biometrics-based systems have some drawbacks, such as universal coverage, implementation difficulties, and accessibility issues. In order to comprehend how users view the system, this thesis examines Aadhaar, India's biometric identification system, as a case study. Enrolling more than one billion people, the system is the biggest biometric identity system

globally. In order to guarantee that state money would be distributed directly and exclusively to people in need, India developed Aadhaar with the dual goals of giving identity to those who were not enrolled in the existing system and ensuring that government databases could communicate with one another. According to the State of Aadhaar (2018), 4.4% of Indian people are not enrolled in Aadhaar for a variety of reasons, despite the app's astounding enrollment statistics. These folks are completely barred from the welfare services for which they qualify because they have no other option. Aadhaar has thus been characterized as both a success and a failure by various academics. In order to structure the analysis, this study will make use of the World Bank's Principles on Identification for Sustainable Development: Toward the Digital Age. With the use of the World Bank's principles, this study will determine what aspects of Aadhaar have worked successfully and what requires improvement. According to the study's findings, people's opinions of Aadhaar were either neutral or favorable when it performed effectively for them. However, individuals were totally shut out of the system when Aadhaar failed to function for them. More efficient alternative authentication techniques are therefore required.

3. Research Methodology

It makes sure that only the legitimate pensioner can access their account and get their pension by using biometric characteristics like fingerprints or facial recognition. Biometric information is more difficult to guess or steal than passwords. The purpose of biometric authentication is to make it easier to use, especially for elderly people who might not be accustomed to complicated authentication techniques. It makes it easier to log in without having to memorize PINs or passwords. Any device that enables biometric authentication, such as PCs or smartphones, can safely access pension details thanks to the system. As a result, there are less delays in pension payments. The likelihood of fraud or illegal access is reduced because biometric information is specific to each person and difficult to duplicate. An easy and safe authentication process is made possible by integration with Auth0. In order to maintain the security of pensioner accounts, Auth0 controls user identities and session management.

4. System Architecture

Integrating biometric authentication technology (such as fingerprints, facial recognition, or iris scanning) to safely authenticate people attempting to access their pension accounts online is known as a Web Biometric Authentication System for Pension Retrieval. To provide safe authentication, pension retrieval, and data management, the system architecture for this type of solution would be composed of several parts, each of which would play a distinct role as shown in Figure 1.

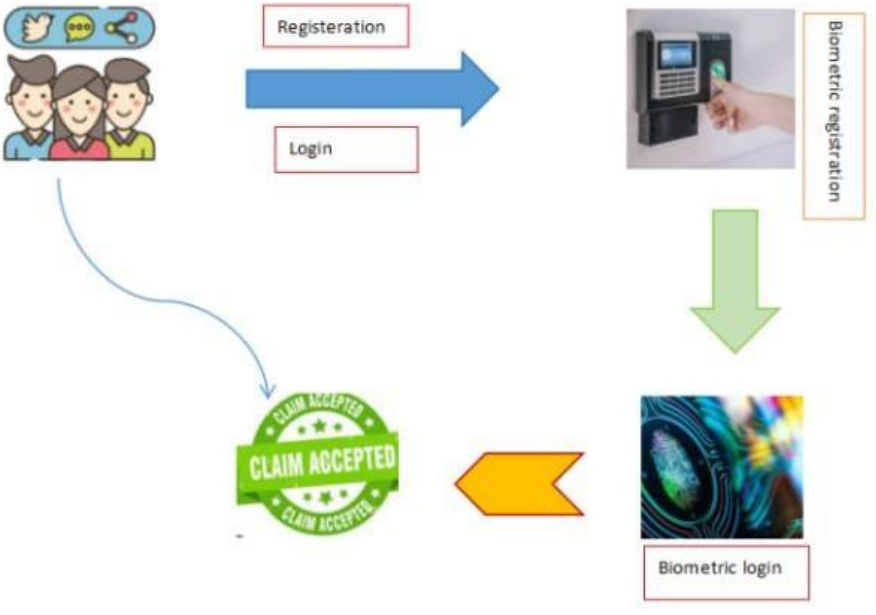

Figure 1. System architecture

5. Modules

- Frontend module
- Backend Module
- Auth0 Integration
- Security Module

5.1 Frontend Module

Authentication, the system retrieves the pensioner's information from the database and shows the amount that will be paid out.

Integration with Auth0: Auth0 manages authentication, guaranteeing that only seniors with permission may access their data.

This module enables the user to use biometric information for authentication and to engage with the web service. The front-end consists of: Pensioners can register their biometric information and authenticate when they want to access their pension using the Biometric Authentication User Interface, which is easy to use and intuitive. WebAuthn () Integration: Gathers biometric information (such as a fingerprint or face) for authentication via the WebAuthn API. Auth0 Integration: For login and session management the front-end interface interacts with Auth0.

5.2 Backend Module

Express.js is used in the back-end module's construction to handle pension-related tasks and authentication: Endpoints for APIs: Once biometric authentication is complete, the back-end makes API routes available for pension retrieval. Pension Data Retrieval: Following authentication, the system retrieves the pensioner's information from the database and shows the amount that will be paid out.

Integration with Auth0: Auth0 manages authentication, guaranteeing that only seniors with permission may access their data.

5.3 Auth () Integration

Secure user authentication is handled by Auth0, which guards against unwanted access to the pensioner's data: User Registration: For safe authentication, pensioners register their biometric information.

Authentication: WebAuthn confirms the pensioner's identity at login, and Auth0 provides a secure JWT token.

Session Management: The pensioner's session is securely managed thanks to Auth0.

5.4 Security Module

WebAuthn Protocol: Guarantees the safe collection, transfer, and validation of biometric information.

SSL/TLS Encryption: To avoid unwanted access or data interception, SSL/TLS is used to encrypt all communications between the client, server, and database.

Token-Based Authentication: Auth0 does not require password storage on the server because it employs JWT tokens for safe authentication and session management.

6. Implementation

Biometric Authentication: The WebAuthn API is used to implement biometric authentication. Pensioners submit their biometric information, which is safely kept in Auth0 and includes fingerprints and facial recognition.

Authentication: The pensioner's biometric information is checked against the records kept in Auth0 when they attempt to log in to the system. Access to the pension account is provided following a successful verification process.

6.1 The module for the back-end:

API Routes: Contains endpoints to manage requests for pension data retrieval following biometric verification.

Data Verification: Retrieves the accurate pension amount from the pension database and verifies the pensioner's eligibility.

Session Management: After the pensioner logs in, secure session management is achieved using JWT tokens.

Auth0 Integration: User authentication is accomplished using the integration of Auth0: Secure Biometric Enrollment: When pensioners register, their biometric information is safely saved in Auth0.

Authentication and Authorization: Auth0 issues a JWT token, which is used to access pension data, after confirming the pensioner's identity during login.

7. Results

To prevent social security fund abuse, an automated technique for identifying deceased beneficiaries makes use of cutting-edge technologies including biometric verification, AI-driven algorithms, and real-time data matching to compare beneficiary information with death databases.

Technology automatically detects and stops payments to deceased people by continuously monitoring the social security database and integrating biometric information, such as fingerprints or facial recognition, during beneficiary registration. By stopping additional payments and guaranteeing that only qualified recipients receive benefits, this lowers the possibility of fraud. Additionally, the system keeps thorough audit trails for accountability and transparency, which eventually improves social security agencies' accuracy, efficiency, and cost savings while guarding against the misappropriation of public funds.

The method frees up resources for more complicated duties by automating the identification of deceased beneficiaries, which lessens the administrative load on social security authorities. Large volumes of data can be processed rapidly and accurately by AI algorithms, reducing human error and guaranteeing that only surviving beneficiaries get payouts. The results obtained on effectiveness of automated beneficiary system is shown in Figure 2.

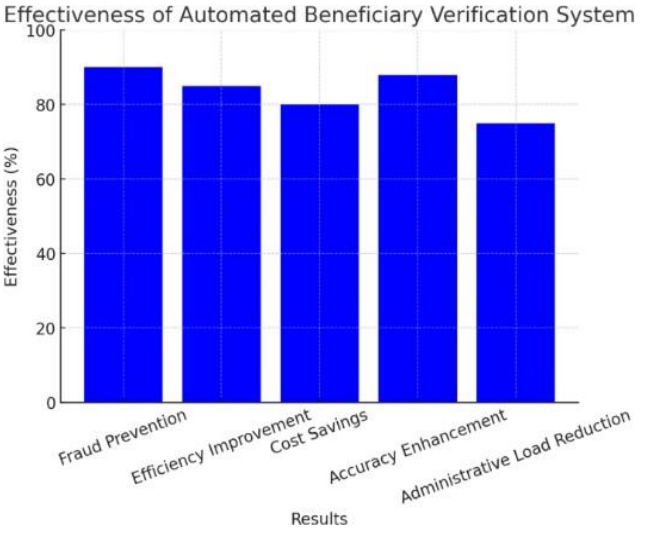

Figure 2. Effectiveness of automated beneficiary system

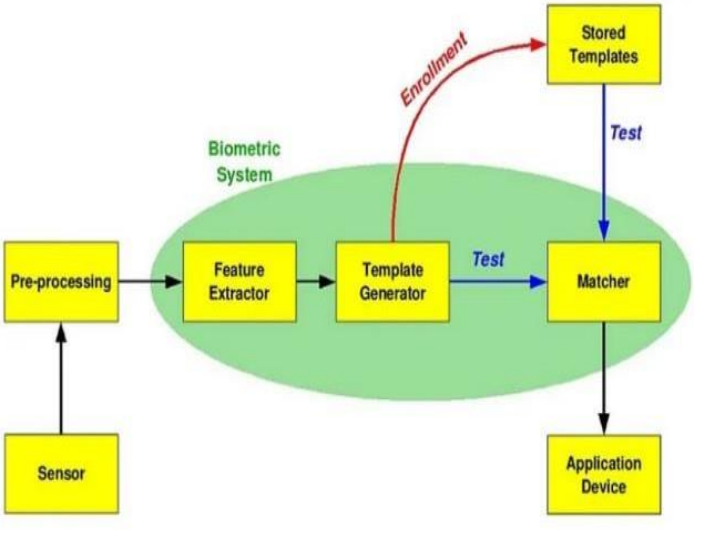

Figure 3. Multi biometric authentication system

By stopping deceased people from receiving benefits, this approach directly addresses social security fund abuse. Additionally, it lessens the possibility of false claims being filed in the names of deceased people. The technique helps conserve important money that would otherwise be stolen by removing the possibility of overpayments.

8. Future Discussion

Multi-Biometric Authentication: For even more secure authentication, future upgrades may allow more biometric techniques shown in Figure 3. Enable pensioners to authenticate using the built-in biometric systems of their devices by expanding support for mobile platforms (iOS, Android).

AI-Based Fraud Detection: Use AI algorithms to identify attempts at illegal access or fraudulent activity.

9. Conclusion

This project improved the security and accessibility of pension benefits for retired people by successfully implementing a biometric authentication system for pension retrieval. One creative and proactive way to combat social security fund abuse is to employ an automated system to identify beneficiaries who have passed away. This approach greatly reduces fraudulent activity and safeguards public funds by ensuring that benefits are only given to qualified individuals through the use of cutting-edge technologies like biometrics, artificial intelligence, and real-time data matching. The solution makes sure that only authorized pensioners can access their pension information by integrating Auth0 for identity and session management and employing biometric authentication (facial recognition and fingerprints).

References

[1] S.J. Grannis, J.M. Overhage, C.J. McDonald, (2002) Analysis of identifier performance using a deterministic linkage algorithm. *In Proceedings of the AMIA Symposium*, 305–309.

[2] E. Owusu-Oware, J. Effah, (2024) Biometric system for protecting information and improving service delivery: The case of a developing country's social security and pension organisation. Information Development, 40(1), 61-74.

[3] Emmanuel C. Omeye, (2021) Design and implementation of tax payment system using fingerprint biometrics and bank verification number. *International Digital Organization for Scientific Research IDOSR Journal of Scientific Research*, 6(2), 20-29.

[4] A. Gelb, C. Decker, (2012) Cash at your fingertips: Biometric technology for transfers in developing countries. *Review of Policy Research,* 29(1), 91-117. https://doi.org/10.1111/j.1541-1338.2011.00539.x

[5] C. Schauder, (2020). Biometric Identification Systems for Welfare Distributions: A Case Study of Aadhaar. *Digital Georgetown.*

[6] A. Zaidi, K. Rake, (2001). Dynamic microsimulation models: a review and some lessons for SAGE. *Simulating Social Policy in an Ageing Society (SAGE)*, 1-40.

Funding

No funding was received for conducting this study.

Conflict of interest

The Author's have no conflicts of interest to declare that they are relevant to the content of this article.