Enhanced Social Network Security System: Integrating Biometric Authentication for Improved User Verification and Privacy Protection

Amaefule I. A., C. I. Ubochi., F.C. Anamelechi

Department of Computer Science, Imo State University, Owerri, Imo State Nigeria

DOI: https://doi.org/10.51584/IJRIAS.2025.100900026

Received: 08 September 2025; Accepted: 14 September 2025; Published: 11 October 2025

ABSTRACT

Social networks are becoming a necessary component of contemporary life, yet security is still a major worry. Conventional password-based authentication methods are susceptible to a number of threats that jeopardize user privacy and data. In order to offer strong user verification and privacy protection, this study suggests an enhanced social network security system that incorporates biometric authentication; through the use of fingerprint scanning. The Enhanced Social Network Security System establishes a biometric authentication system that restricts access to vital websites, networks, and web-based applications to those who are approved, as used in this study which protect user biometric data integrity; when compared to conventional password-based systems. The suggested solution exhibits better security and usability. According to experimental results, erroneous acceptance and rejection rates have significantly decreased, guaranteeing precise user verification. The System offers social networks a practical and safe authentication solution that safeguards user information and privacy. The use of biometric authentication improves social networks' overall security posture and increases their resistance to online attacks.

Keywords: Biometric authentication, social network security, user verification, privacy protection, machine learning.

INTRODUCTION

Social network communication has grown in popularity over the last few years, because of its widespread use; it is challenging to identify the shortcomings of the current system and create a fresh, enhanced framework that can yield superior outcomes. Members expose a significant portion of their private life to security risks by using social networking sites to publish posts, videos, photos, and many other types of content. The dependability of current security methods in extensively networked social media is called into doubt due to their shortcomings. In the current situation, password leaks and unauthorized authentication are leading to cybercrimes [1].

Passwords are the foundation of most social network authentication techniques; however, they may be shared, forgotten, phished, or compromised as is presently the case. Social networks that rely solely on user names and passwords may be giving unauthorized people access to private communications, sensitive information, and online activities.

Most websites are merely secured with user names and passwords. Websites for online banking or investing, online auctions, credit-related websites, social networking sites, and more. Stronger security measures are required, as evidenced by several papers and recent research.

By utilizing your distinct fingerprint and implementing a biometric layer of protection, important websites, networks, and web-based apps can only be accessed by authorized users. Biometrics are taking the place of less safe and practical authentication technologies among consumers and companies of all sizes. Biometrics used to be too costly to be considered and too hard to implement. [2].

This study makes a compelling case for the use of biometrics as an authentication factor for social media websites, guaranteeing that only authorized users can access vital information and enabling the tracking and capture of criminal elements or malicious users who use social media's widespread use as a communication tool to indulge in their vices.

The Beneficial Impacts of Social Network

Generally, collaborative media creation and sharing on a sizable scale are referred to as social media. Various users' communication demands are met by social media. Computer interactions make communication easier by enabling users to conveniently stay in contact with friends and family, hear about social events, and discover what other users are up to [3].

Social networks facilitate content sharing, which is crucial for fostering a feeling of community and shared identity, claims [4]. Sharing textual, video, or audio information on social media platforms that depicts or reflects a person's lifestyle and community experiences enables others to get to know them. The key takeaway from the aforementioned function is that social media fosters ongoing communication between people who share similar interests and may use it for both solitary and group experiences.

[5], makes the case that social media use indicates that these websites have developed into crucial instruments for managing connections with a vast and frequently diverse network of individuals who offer social support and act as channels for helpful information and other resources, which he summarizes as social capital.

It is important to note that social media serves commercial purposes in addition to promote social relationships and ongoing connectedness between people and peers.

[6] notes that in many economic transactions, the social environment is a main motivator of behaviors and results rather than a secondary one. Social networks have a major role in helping people find employment, and they also have an impact on decisions about what to buy, how much education to seek, and whether or not to commit crimes. Because of the broad recognition of the value of integrating economic activity into social networks, researchers, businesspeople, governments, and individuals have begun to use social networks to quickly and widely approve and embrace policies, decisions, and concepts.

All things been considered, shows that social networks have revolutionized how we interact, communicate, and obtain information, providing a wealth of advantages for people, groups, and society at large.

LITERATURE REVIEW

Depending on the individual, the social network might signify numerous things. Some people use social media platforms to advertise their companies, while others utilize them for a variety of other objectives, such as education and amusement. As a result, there are various perspectives on the idea of a social network. Social networking sites are online groups of people who either share interests and activities or are curious about the interests and activities of others, according to [7]. They usually give users a range of ways to communicate, including file sharing, blogging, discussion groups, video, phone, email, chat, and messaging. [8] adds that social networks are web-based platforms that enable people to engage in a variety of activities. In a bounded system, it first enables users to create a public or semi-public profile; then, it helps them to list other users with whom they are connected; and lastly, it enables them to view and navigate both their own and other users' connections lists.

The degree of worry over security vulnerabilities on social networking sites has increased geometrically over time. Others have lost their hard-earned money and other belongings, and many have been enticed to their deaths. Some people experienced a decline in their job as a result of a campaign of defamation on social media. Unfortunately, because of security flaws and ineffective methods of online user verification, the majority of these offenses remain unpunished. This section’s goals are to outline various security problems and worries related to social networking sites in an effort to provide a workable solution. The problem of social networking sites in relation to user account access and privacy is examined in this paper. As stated by [9],[10], criminals are outpacing the advancement of security-ensuring technologies. These criminals target both people (via social engineering, Trojan horses, and phishing) and technology (through malware and denial of service assaults on digital data, systems, and hardware). [10] recommended that in order to create suitable rules and safety and confidentiality measures, it is necessary to fully comprehend the elements pertaining to social networking security.

Phishing is one of the most prevalent and high-ranked security flaws and assaults on social networking platforms. Phishing is defined in A Survey of Various Security Issues in Online Social Networks as an attack technique whereby the attackers gain the victim's sensitive information [11]. Phishing is when a hacker creates a phony website that mimics an authentic one. The victim will receive a notification from the attacker stating that they must authenticate their profile or risk having it removed. When the victim visits the particular phony website, it will request the individual to supply the sensitive data and login and password of the victim. Majority of the time, the attacker succeeds because consumers are clueless; if successful, this attack enables the attacker to get direct access to the user's account and important data, such as all posts and changes that are limited to certain users, using the user's log-in credentials to accomplish some goal against the user's personality, which leads to identity theft.

One of the biggest concerns on social networking platforms is identity theft. Social media users must exercise caution and vigilance since identity theft is a very significant problem. The goal of identity theft is to post or transmit communications on someone else's behalf without that person's knowledge or consent. Some individuals are compelled to remove their profiles as a result of identity theft because of the subsequent shame, according to [12]. Fake profiles are occasionally created, and the real user is unaware that the attacker is updating and behaving in a shameful manner.

[13], listed malware, viruses, and frauds as problems affecting social network users. Individuals see a plethora of posts, messages, and comments on their walls, web page, or profile as soon as they check in. The user may get these communications as spam or as a targeted assault. Users become susceptible and fall prey to such attacks when they are unable to detect or recognize such communications. Identity theft happens when malware is introduced into the user account and accounts are compromised, resulting in the recovery of personal data. As a result, assaults on social media platforms have made individuals less confident in the system. The chat between the two individuals cannot be trusted since one of the accounts may have become compromised or may be the target of future attacks, which would violate the conversation's privacy (by leaking it).

The problem of each member's legitimacy on social networking sites might be linked to identity theft. There is no way for the social network to confirm the personal information of people who have registered. Additionally, it has been noted that a current user may create or possess additional accounts, resulting in many accounts belonging to the same person with either the same or distinct identities.

Also, criminally inclined second party can access and control an account without the account owner's knowledge by simply obtaining the username and password through any hacking methods; which necessitates the need for additional verification or checks.

Because of these problems, a higher degree of authentication is now required in order to access social networks. A more distinctive and uncompromising approach must be added to or substituted for the traditional username and password way of accessing each account. a method that ensures the owner of the account is present or has given permission before any online activity can begin. This method will also guarantee that every action taken on social media can be linked to an actual, living person and that there is a means of verifying the problem of multiple accounts. Because of this, this study examines the authentication method in social networking platforms by combining biometrics data collection, paying particular focus to the fingerprint verification and authentication method.

METHODOLOGY

Fingerprint-based biometric authentication is integrated into the Enhanced Social Network Security System to offer strong user verification and privacy protection. The solution is intended to solve the security and authentication problems that social network users face. By incorporating biometric data collection during registration, the new system will be able to handle the security difficulties and password authentication concerns that social network users experience, while keeping in mind the description and problems of the current system. This will guarantee that no current user may create a new account. This will stop problems with a single user having several accounts and the criminal inclinations it encourages.

Three tiers of the system architecture will be used in its design: the Presentation tier, which will collect fingerprint data; the Middle (Logic) tier, which will extract and match features; and the Data tier, which will collect biometric authentication.

i. ***Presentation Tier:*** The user interface is another name for the Presentation tier. The Graphical User Interface, which enables user interaction with the system, is displayed. The individual's fingerprints are collected using a fingerprint sensor, processed to improve quality, eliminate noise, and extract distinctive traits, after which a fingerprint pattern is made from the processed fingerprint picture.

ii. ***The Middle layer:*** This layer manages the program, makes rational choices, and carries out the duties that the system's users have assigned it. Additionally, it serves as a client between the system's other levels. Here, distinctive properties, such minute details, are taken from the fingerprint template in order to do feature extraction and matching. The matching method compares the retrieved characteristics to a database of fingerprint templates that have been saved.

iii. ***The Data Tier:*** This Layer is in charge of the system's database. It comes with a program and storage that let users access, modify, and handle the data kept in the system. A fingerprint sensor is used to scan the user's fingerprint when they seek permission to use the social site. The fingerprints are then compared to a saved fingerprint template, and if they match, the user is given access to the social network. To avoid unwanted access, data on fingerprints are encrypted. The two diagram in fig.1 and fig. 2, illustrate fingerprint biometrics authentication for improved user verification and privacy protection.

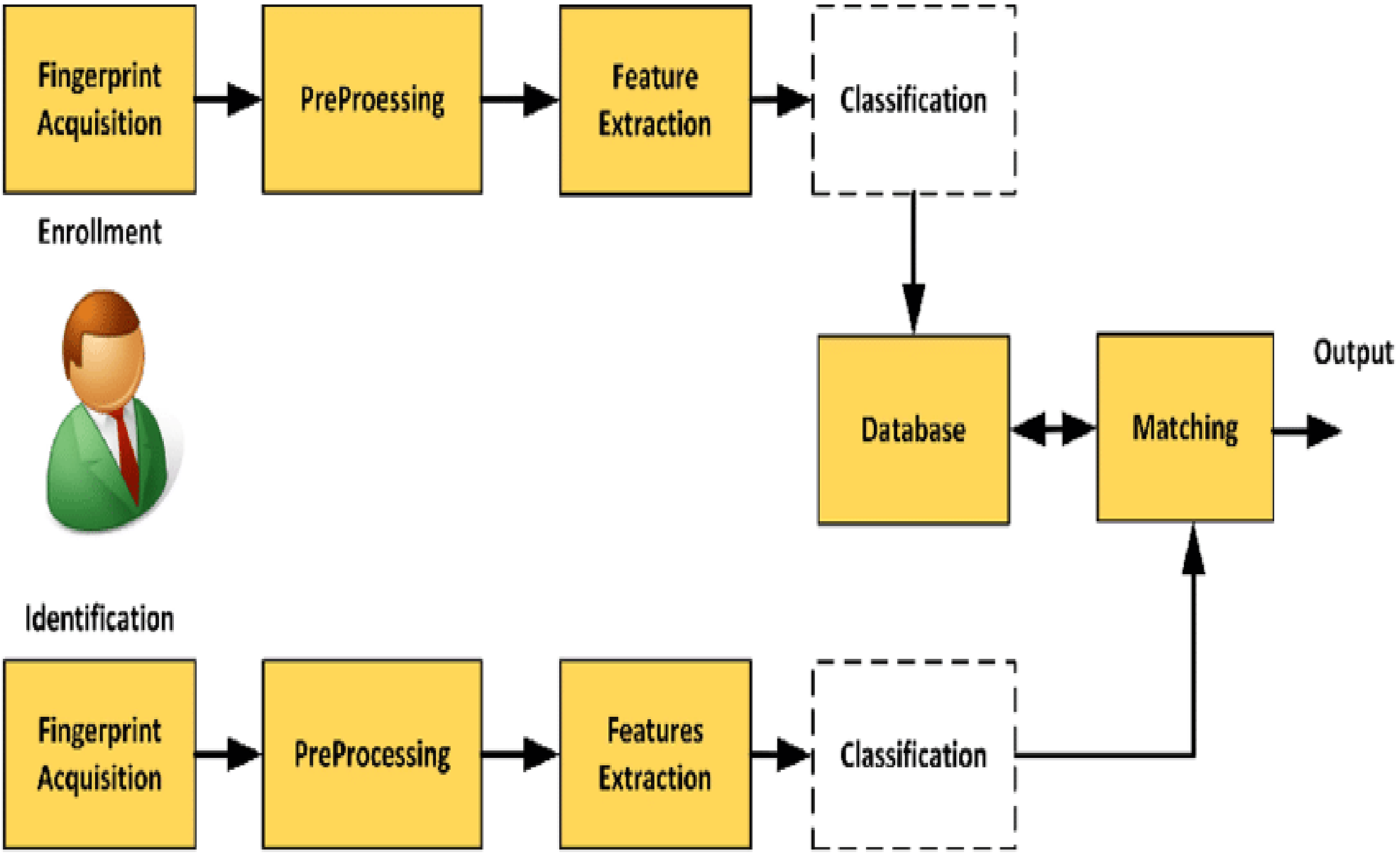

Fig. 1**:** Diagram of fingerprint identification system (basic components) [14].

The flowchart of fingerprint biometrics authentication for improved user verification and privacy protection.

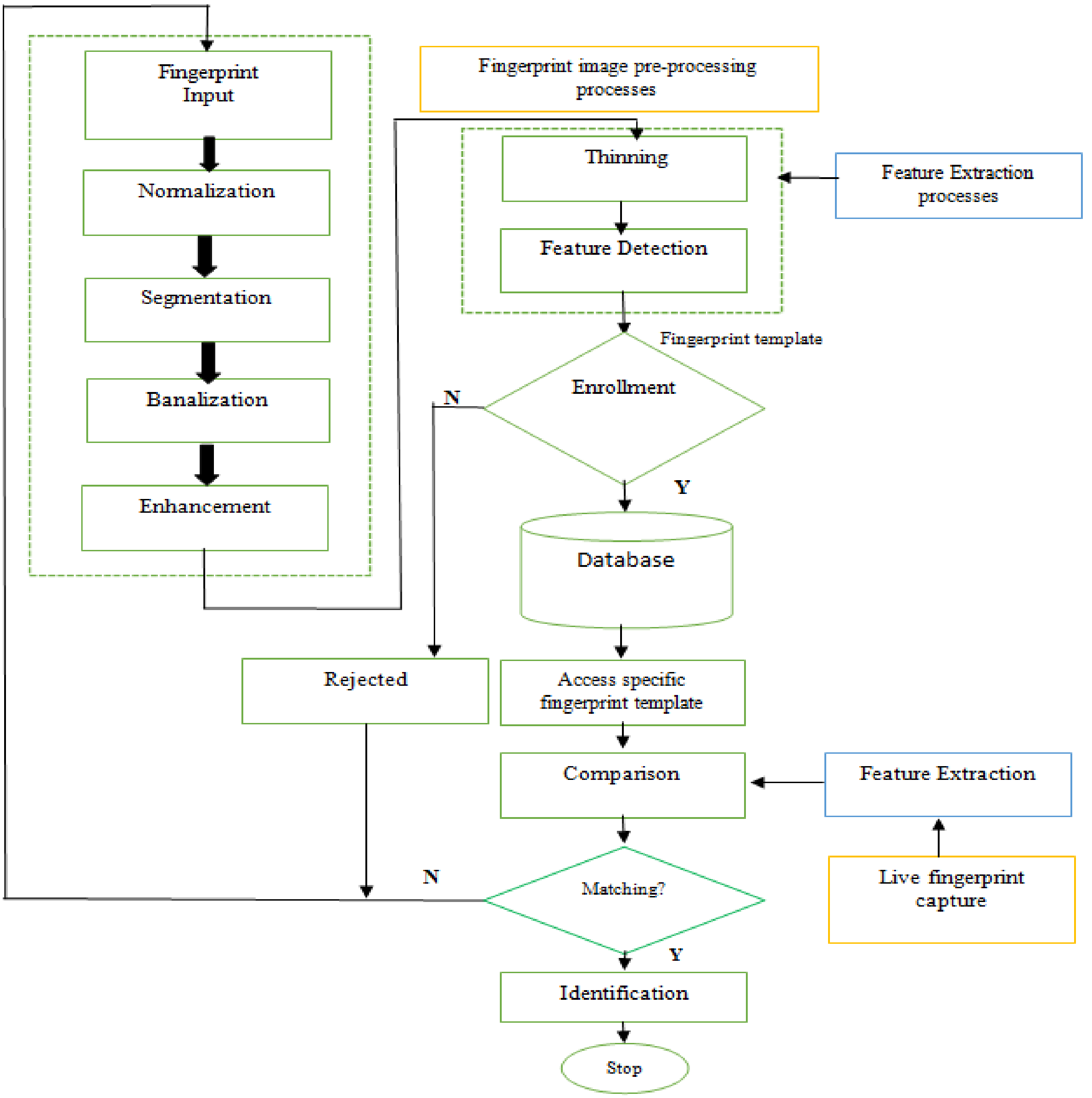

Fig. 2: The flowchart of fingerprint biometrics authentication for improved user verification and privacy protection.

CONCLUSION

By incorporating biometric authentication, the Enhanced Social Network Security System offers a reliable and practical way of improving verification of users and guarantee confidentiality. This system uses fingerprint recognition technology to provide a safe and convenient substitute for conventional password-based authentication techniques. By lowering the possibility of password-related assaults and data breaches, biometric identification improves security. Fingerprint recognition offers a quick and easy login procedure that does away with the need for passwords. Sensitive user data is protected by the system's encryption and secure storage features, which improves privacy protection. An important advancement in safeguarding user information and maintaining the integrity of social networks is the Enhanced Social Network Security System. Prioritizing security, simplicity, and consumer trust is crucial as technology develops further.

ACKNOWLEDGMENT

Sincere gratitude is extended to the TetFund for providing financing and enabling the successful completion of the study, and also to the Vice Chancellor of Imo State University, Owerri for promoting teamwork in research at the university.

REFERENCE

1. Sharma, S. and Soldhi, J.S. (2014). Implementation of Biometric Techniques in Social Networking sites. International Journal of Security and its Applications. Volume 8.No. 6. Pp. 51-60.
2. Dabbour, M., Alsmadi, I., and Emad, A. “Efficient Assessment and Evaluation for Websites Vulnerabilities Using SNORT”. *International Journal of Security and Its Applications* Vol. 7, No.1, January, 2013.
3. Sponcil, M. and Gitimu, P. Use of social media by college students: Relationship to communication and self-concept. Journal of Technology Research
4. Collin, P., Rahilly, K., Richardson, I. & Third, A. (2011). The Benefits of Social Networking Services: A literature review. Cooperative Research Centre for Young People, Technology and Wellbeing. Melbourne. ISBN: 978-0-9871179-1-5.
5. Steinfield, C., Ellison, N., Lampe, C. and Vitak, J. (2012). Online Social Network Sites and the Concept of Social Capital. Frontiers in new Media Research, New York: Routledge, pp 115-131.
6. Matthew O. Jackson. (2007). The Study of Social Networks in Economics. Prepared for The Missing Links: Formation and Decay of Economic Networks.
7. Singh, V., Beniwal, Bulbul, D., and Tomer, J. (2015). Why Adolescents Use Social Networking Sites: A Gender-based Analysis. Afro Asian Journal of Social Sciences Volume VI, No 1. Quarter I. ISSN: 2229 – 5313
8. Dewing, M. (2012). Social Media: An Introduction. Parliamentary and Research Service, Canada. Publication No: 2010-03-E, 3 February 2010. Revised 20 November 2012.
9. Luo, X. & Liao, Q. (2007). Awareness Education as the key to Ransomware Prevention. Information Security Journal, 16(4), 195-202.
10. Mehdi, S. & Arbi, G. (2104). Security Requirements in Social Networks. Issues in Information Systems Volume 15, Issue I, pp. 81-87.
11. Joe, M. &Ramakrishnan, B. (2014). A Survey of Various Security Issues in Online Social Networks. International Journal of Computer Networks and Applications Volume 1, Issue 1, November – December.
12. Gangopadhyay, S. & Dhar, D. (2014). Social Networking Sites and Privacy Issues Concerning Youths. Global Media Journal-Indian Edition ISSN 2249 – 5835 Summer Issue/June 2014/Vol. 5/No. 1
13. Okurumeh, O. & Ukaoha, K. (2015) Information Security Issues Surrounding Use of Social Media Networks in Organizations: An Appraisal. Journal of Emerging Trends in Engineering and Applied Sciences (JETEAS) 6(3): 227- 232
14. Awad, Ali Ismail. (2012). Machine Learning Techniques for Fingerprint Identification: A Short Review.: International Conference on Advanced Machine Learning Technologies and Applications. DOI:10.1007/978-3-642-35326-0_52.