Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 14, No. 3, 2024

Biometric and Geographic Information-based Identity Authentication Method

Xiaopeng Yang

National Key Laboratory of Advanced Communication Networks, Shijiazhuang, Hebei, China

Abstract: With the ongoing advancements in computer technology and mobile internet, mobile payment has become an integral component of daily life. Identity authentication technology serves as a critical measure to ensure the security of mobile payments. This paper addresses the issue of low security associated with single-factor identity authentication while highlighting the substantial overhead involved in multi-factor authentication methods. We propose a novel identity authentication method that integrates biometric data and geographic information. In this framework, the identity authentication server first performs system initialization, configures system parameters, and stores them securely. Subsequently, the identity authentication client submits an authentication request to the server and completes its registration process. Finally, the server processes this request from the client, conducts user identity verification, and returns an authentication result. This approach effectively mitigates risks posed by attackers attempting to falsify biometric data or geographic information during the identity verification process and offers robust services for biometric- and geography-based identity authentication.

Keywords: Mobile Payment; Identity Authentication; Biometric Features; Geographical Location.

1. Introduction

Authentication serves as the cornerstone for ensuring the trustworthiness and reliability of user identities. Single-factor authentication methods exhibit lower security due to vulnerabilities associated with the potential leakage of authentication factors, whereas multi-factor authentication approaches enhance both security and reliability by integrating multiple verification elements. Presently, several identity authentication methods leverage biometric data and geographic location information to safeguard user identity [1,2,3]. While these approaches successfully combine various factors, they often fail to validate the reliability of each individual authentication element. Consequently, attackers may exploit technical means to fabricate biometric and geographic location data, thereby compromising the integrity of the authentication process and jeopardizing system security.

This paper identifies the limitations of current technologies and introduces a novel identity authentication method that integrates biometric data and geographic information, with its advantages primarily evident in the following three aspects:

Ensures the reliability of geolocation information in the user authentication process.

By authenticating the fingerprint of the user's authentication device and subsequently determining the actual location for identity verification based on the device's deployment site, this approach mitigates the risk of attackers evading geographic location authentication through technical means, such as modifying IP addresses or location data when directly verifying user locations via IP address or GPS devices. This method ensures the reliability of users' geographic location information throughout the identity authentication process.

(2) Ensures the reliability of biometric information throughout the user authentication process.

By initially authenticating the device fingerprint and geographic information, followed by biometric authentication, this approach ensures that the user's biometric data is initiated exclusively through the designated identity authentication client. This method mitigates the risk of attackers collecting users' biometric information via alternative channels such as social networks and generating synthetic biometric data capable of passing verification by biometric identification systems utilizing artificial intelligence algorithms, thereby ensuring the reliability of the biometrics-based identity authentication process.

(3) Minimizes the communication overhead associated with the identity authentication process.

The device fingerprint and the user's biometric information are encapsulated within a single image, eliminating the need for additional data such as IP addresses or GPS locations during the authentication process, thereby minimizing communication overhead in identity verification.

2. Related Work

The evolution of identity authentication technology has transitioned from rudimentary password systems to more sophisticated password mechanisms, and subsequently to biometric and multi-factor authentication methods, reflecting substantial advancements in the field [4].

Biometric recognition technology is an authentication method that leverages the unique biological characteristics of users, such as fingerprints, facial features, and irises [5]. This approach eliminates the need for users to explicitly input authentication information, resulting in expedited authentication processes; however, it remains susceptible to numerous security vulnerabilities. Yuan [6] pioneered a lightweight authentication protocol for wireless sensor networks utilizing fingerprint-based biometric factors; nevertheless, this system was unable to withstand offline password guessing attacks, privileged insider threats, and gateway node impersonation attacks while failing to safeguard query results. Bontrager et al. [7] reported a successful intrusion rate of up to 75% against advanced fingerprint authentication systems by employing adversarially generated fingerprint images through generative adversarial networks. Similarly, Erdogmus et al. [8] successfully compromised multiple facial recognition

systems by constructing tailored datasets of custom 3D face masks. Regarding iris recognition systems, Czajka et al. [9] developed a textured eye model designed to mimic human irises, achieving a remarkable 95% success rate in breaching iris authentication systems based on support vector machines.

Multi-factor authentication enables the verification of user identity across multiple dimensions, offering significant security advantages. Biometric features frequently serve as one of these factors. In various schemes, biometric information is recognized as a critical component [10]. Pang et al. [11] utilize a diverse array of data—including smartphone location, applications, Bluetooth connectivity, WiFi access, SMS messages, and phone calls—to authenticate users, achieving an impressive accuracy rate of 98.5%. Nevertheless, multi-factor authentication schemes are often characterized by considerable authentication overhead.

3. Proposed solution

The identity authentication system, which is based on biometric and geographic information, comprises two primary components: an identity authentication server and an identity authentication client, as illustrated in Figure 1.

Identity Authentication Server: This component is responsible for system initialization and facilitates the registration process for both identity authentication clients and users. It stores pre-defined system parameters, user identification information, biometric data, and acceptable geographic ranges for authentication. Additionally, it maintains records of identity authentication client identifiers, device fingerprint information, and their respective geographic locations. The server processes user authentication requests, computes the corresponding authentication results, and subsequently returns these results to the identity authentication client.

Identity Authentication Client: This component captures image data to transmit registration requests to the identity authentication server and subsequently receives the corresponding registration results. Additionally, it gathers image information to submit authentication requests to the server, from which it also obtains the respective authentication outcomes.

The system authentication workflow is illustrated in Figure 2.

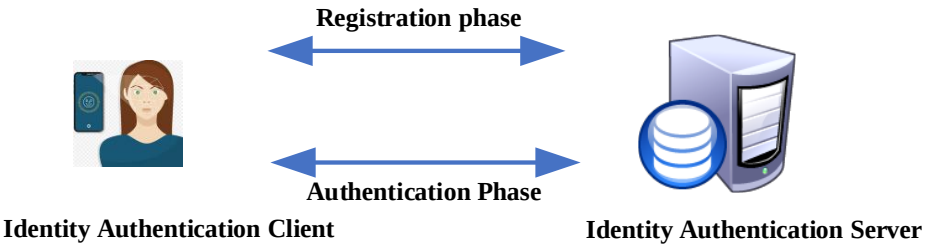

Figure 1. System Architecture Diagram

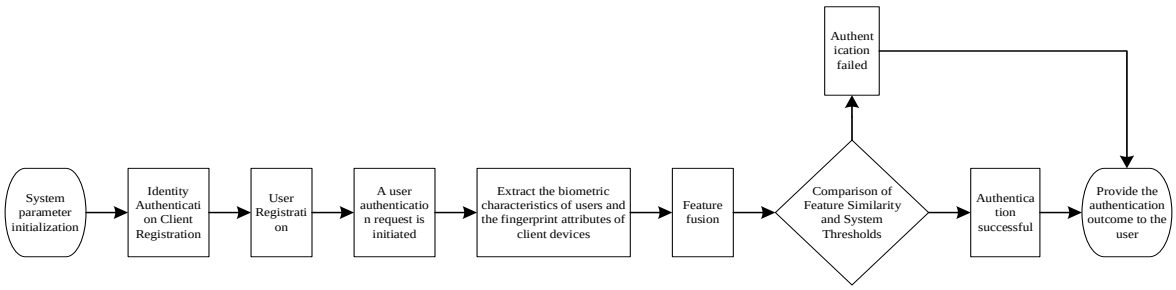

Figure 2. Schematic Representation of the Identity Authentication Process Utilizing Biometric and Geographic Information

(1) **System parameter initialization**

(1a) The identity authentication server establishes the biometric similarity threshold as Δ_1 and the device fingerprint similarity threshold as Δ_2 for the system, subsequently storing these values.

(2) Identity Authentication Client Registration

(2a) The identity authentication client c captures an image F_c of its device fingerprint using its camera and transmits the acquired image F_c, along with the identity authentication client's identifier F_c and the geographic location information r_c associated with the deployment of the identity authentication client, to the identity authentication server, thereby initiating a request for registration of the identity authentication client.

(2b) Upon receiving the registration request submitted by the authentication client, the authentication server extracts image F_c, the identifier ID_c of the authentication client, and the geographic location information r_c pertaining to the deployment of the authentication client.

(2c) The authentication server extracts the device fingerprint $T_{c1} = (t_{c11}, t_{c12}, \cdots, t_{c1m})$ of the authentication client from the registration request image F_c, wherein t_{c1i} denotes the value of the i-th dimension of the device feature fingerprint.

(2d) The authentication server establishes an association between the client identifier ID_c, the device fingerprint

ID_c of the client's device, and the geographic location information r_c, subsequently storing this data.

(2e) The authentication server communicates to the authentication client c that the registration process has been successfully completed.

(3) User Registration

(3a) User u captures an image F_u that encompasses their biometric information and transmits it, along with their identity identifier ID_u, the corresponding biometric image, and the defined geographic range for authentication R_u to the identity authentication server in order to initiate a user registration request.

(3b) Upon receiving the authentication request submitted by the user, the authentication server extracts the user identifier ID_u, the image F_u containing the user's biometric features, and the defined geographic range for authentication R_u.

(3c) The identity authentication server extracts the user's biometric features from the biometric extraction image F_u, where t_{u1i} denotes the value of the i-th dimension of the device feature fingerprint $T_{u1} = (t_{u11}, t_{u12}, \cdots, t_{u1n})$.

(3d) The identity authentication server establishes an association between the user's identification ID_u, their biometric features T_{u1}, and their defined geographic range for authentication R_u, subsequently storing this information.

(3e) The authentication server transmits a confirmation of successful registration to user u.

(4) Identity authentication

(4a) A registered user u, having completed the identity authentication process, captures the user's image F_{uc} via a client c that has also undergone identity authentication. The user ID ID_u, client ID ID_c, and the image F_{uc} obtained through the authenticated client 6 are then transmitted to the identity authentication server to initiate an identity authentication request

(4b) Upon receiving an authentication request from user u, transmitted by the authentication client c through image F_{uc}, the authentication server subsequently extracts the device fingerprint $T_{c2} = (t_{c21}, t_{c22}, \cdots, t_{c2m})$ of the authentication client c from image F_{uc}, where t_{c2i} denotes the value of the i-th dimension of device fingerprint T_{c2}; concurrently, the authentication client captures the user's biometric feature $T_{u2} = (t_{u21}, t_{u22}, \cdots, t_{u2n})$ for authentication, with t_{u2i} indicating the value of its i-th dimension.

(4c) The authentication server extracts the registered features T_{u1} of user u based on the user's identifier ID_u, along with the permissible authentication geographic range R_u; it further extracts the device fingerprint T_{c1} of authentication client c according to the client's identifier ID_c, as well as the deployment geographic location r_c.

(4d) The authentication server evaluates the similarity between device fingerprint T_{c1}, acquired during the registration phase of the authentication client, and device fingerprint T_{c2}, obtained during the authentication phase, to ascertain whether it meets predefined criteria. If the similarity satisfies these criteria, it is concluded that the user has initiated an authentication request through a legitimate authentication client c, with the user's current location for this request being identified as deployment location r_c of said client; conversely, if the similarity fails to meet these criteria, it is determined that the user's authentication pathway is illegitimate. In such cases, the server returns an authentication failure notification to the user and terminates the authentication process.

(4e) The authentication server assesses the reasonableness of location r_c from which user u initiates the authentication request; if deemed reasonable, it is concluded that the user has successfully passed the geographic information-based authentication. Conversely, if deemed unreasonable, it is determined that the user has failed to pass this form of authentication, prompting the server to return an authentication failure notification to the user and terminate the authentication process

(4f) The identity authentication server evaluates the similarity between biometric feature T_{u1}, recorded during the user registration phase, and biometric feature T_{u2}, captured during the authentication phase, to ascertain whether it meets the established criteria. If it does, the user is considered to have successfully passed the biometric-based authentication, and a notification of successful authentication is returned to the user. Conversely, if it does not meet these criteria, the user is regarded as having failed this form of authentication; consequently, an authentication failure notification is sent to the user and the process is terminated.

4. Conclusion

This paper identifies the limitations of current technologies and proposes a novel identity authentication method that integrates biometric features with geographic information. By employing cross-verification of multiple factors, this approach facilitates multi-factor authentication of user identity, thereby enhancing the security of the authentication process while simultaneously reducing communication overhead.

References

[1] Lyastani S G , Schilling M , Neumayr M ,et al.Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication[C]//2020 IEEE Symposium on Security and Privacy (SP).IEEE, 2020.

DOI:10.1109/SP40000.2020.00047.

[2] Camenisch J , Lehmann A , Neven G .Optimal Distributed Password Verification[C]//Acm Sigsac Conference on Computer & Communications Security.ACM, 2015:182-194.

DOI:10.1145/2810103.2813722.

[3] Weinshall D .Cognitive authentication schemes safe against spyware[J].IEEE, 2006.

DOI:10.1109/SP.2006.10.

[4] He, Hui Y .Research on the Network Security and Identity Authentication Technology[J].Advanced Materials Research, 2014, 926-930:2819-2822.

DOI:10.4028/www.scientific.net/AMR.926-930.2819.

[5] Palma D , Montessoro P L .Biometric-Based Human Recognition Systems: An Overview[J].Recent Advances in Biometrics [Working Title], 2022.

DOI:10.5772/intechopen.101686.

[6] He D , Gao Y , Chan S ,et al.An Enhanced Two-factor User Authentication Scheme in Wireless Sensor Networks[J].Ad Hoc & Sensor Wireless Networks, 2010, 10(4):361-371.

DOI:10.1016/j.adhoc.2009.05.002.

[7] Bontrager P , Togelius J , Memon N .DeepMasterPrint: Generating Fingerprints for Presentation Attacks[J]. 2017.

DOI:10.48550/arXiv.1705.07386.

[8] Erdogmus N , Marcel S .Spoofing Face Recognition With 3D Masks[J].IEEE Transactions on Information Forensics and Security, 2014, 9(7):1084-1097.

DOI:10.1109/TIFS.2014.2322255.

[9] Ferrero R , Gandino F , Montrucchio B ,et al.On gait recognition with smartphone accelerometer[J].IEEE, 2015.

DOI:10.1109/MECO.2015.7181946.

[10] Yang D , Yang B .A biometric password-based multi-server authentication scheme with smart card[J].IEEE[2024-10-17].

DOI:10.1109/ICCDA.2010.5541128.

[11] Pang Xiaojian, Yang Li, Liu Maozhen, et al. Mineauth: mining behavioural habits for continuous authentication on a smartphone[C]//The 24th Australasian Conference on Information Security and Privacy. Christchurch: Springer Press, 2019: 533-551.