International Journal of Information and Cybersecurity

Int. J. Inf. Cybersec.-2020

Cloud-Based Biometric Authentication Techniques for Secure Financial Transactions: A Review

Anusha Bodepudi
Staff Engineer, Intuit, Plano, TX, USA,
Anusha_bodepudi@intuit.com

Manjunath Reddy
Customer Engineering Lead, Qualcomm , San diego, CA, USA,
reddymanjushari@gmail.com

Abstract

As financial transactions increasingly shift to online platforms, the need for robust authentication methods has become paramount. Cloud-based biometric authentication techniques have emerged as a promising solution to address security concerns and improve user experience. This research explores common cloud-based biometric authentication techniques, including fingerprint authentication, facial recognition, voice recognition, iris recognition, and behavioral biometrics. By leveraging cloud computing technology, these techniques provide a scalable, flexible, and secure environment for storing and processing biometric data and authentication algorithms. The research outlines the process of cloud-based biometric authentication for financial transactions, starting from the enrollment phase, where users securely register their biometric data. Subsequently, during an authentication request, the system captures biometric data through the user's device, encrypts it, and transmits it securely to the cloud server. The received biometric data

is then matched against the pre-registered data stored in the cloud, and the system determines the authentication decision. If successful, the financial transaction is authorized, allowing users to proceed with their desired actions. Cloud-based biometric authentication offers several benefits for financial transactions, including enhanced security due to the difficulty of replicating biometric traits, convenience by eliminating the need to remember multiple passwords or PINs, reduced fraud risk, scalability to accommodate growing user bases, and real-time authentication capabilities.

Keywords: *Cloud-based biometric authentication, Financial transactions, Fingerprint authentication, Facial recognition, Behavioral biometrics*

Introduction

Biometric authentication has emerged as a highly secure and reliable method of granting access to devices and systems. It operates by comparing the biometric features of an individual with those stored in a database, and only when a match is found, access is granted. The uniqueness of biometric characteristics, which encompass physical and biological traits specific to each person, adds a robust layer of security to the authentication process.

The process of biometric authentication begins by capturing and recording the biometric data of authorized users [1]. This data, such as fingerprints, iris patterns, facial recognition, voiceprints, or even DNA samples, is then securely stored in a centralized database. When a user attempts to gain access to a device or system, their biometric features are captured and compared against the stored data. If the parameters closely match, access is authorized; otherwise, the user is denied entry.

The implementation of biometric authentication is not limited to specific environments but can be utilized in various physical settings. For example, it can be employed at the entrances of buildings, doors, and gates, ensuring that only authorized personnel can enter secure areas. Biometric authentication is also extensively used in high-security locations like server rooms, military bases, airports, and ports [2].

In financial institutions, biometrics authentication has emerged as a highly effective and secure method for verifying the identity of individuals. Unlike traditional methods such as passwords or PINs, biometric authentication relies on unique physiological or behavioral characteristics, making it significantly more resistant to fraud and unauthorized access. Financial institutions have increasingly adopted biometric solutions, recognizing their potential to enhance security, streamline user experiences, and reduce operational costs.

By leveraging distinctive biometric markers such as fingerprints, iris patterns, facial features, voiceprints, and even behavioral patterns like typing speed, institutions can confidently verify the identity of users with a high degree of certainty [3]. This level of precision significantly mitigates the risk of identity theft and impersonation, a prevalent concern in the financial sector. Biometric authentication systems excel in offering a seamless user experience, facilitating swift and convenient access to financial services. Gone are the days of remembering complex passwords or carrying multiple identification cards. Biometric technologies empower customers to access their accounts with a simple scan or recognition of their unique biometric attributes [4]. This not only expedites the authentication process but also increases customer satisfaction, leading to higher user engagement and loyalty.

The integration of biometrics in financial institutions contributes to robust security protocols and compliance adherence [5]. Given the ever-evolving nature of cyber threats and regulatory requirements, traditional authentication methods often fall short in providing adequate protection. Biometrics, on the other hand, offer an added layer of security that is difficult for malicious actors to bypass. Moreover, these systems can be designed to comply with industry regulations and standards, ensuring data protection and privacy. biometric authentication significantly reduces the incidences of fraud and financial crimes, saving financial institutions substantial losses in terms of money, reputation, and customer trust. Biometric markers are unique and cannot be easily replicated, minimizing the risk of fraudulent transactions and unauthorized account access. Additionally, real-time monitoring and analysis of biometric data can raise red flags for suspicious activities, enabling institutions to take immediate action to prevent potential threats.

The utilization of cloud computing for biometrics authentication in financial institutions has brought about significant advancements in security, scalability, and cost-effectiveness. With cloud computing, financial institutions can seamlessly integrate and deploy biometric authentication systems, offering a robust and reliable method for verifying user identities.

Cloud computing provides financial institutions with the ability to store and process large volumes of biometric data securely. Biometric authentication systems generate and analyze vast amounts of data, including fingerprints, facial scans, and voiceprints. By utilizing cloud storage and computing capabilities, financial institutions can efficiently manage this data, ensuring its availability and accessibility while maintaining stringent security measures. Cloud-based solutions also enable real-time synchronization of biometric data across multiple devices and

locations, facilitating seamless user experiences and reducing the risk of data loss [6].

Moreover, cloud computing offers unmatched scalability for biometric authentication systems in financial institutions [3], [7]. The demand for authentication services can fluctuate significantly, with peak periods requiring increased computational resources. Cloud-based infrastructures provide the flexibility to scale resources up or down dynamically, ensuring optimal performance and user experience [8]. This elasticity eliminates the need for financial institutions to invest in and maintain dedicated hardware, resulting in cost savings and increased operational efficiency.

Additionally, cloud computing enhances the overall security posture of biometric authentication in financial institutions. Cloud service providers typically implement robust security measures, including encryption, access controls, and intrusion detection systems, to protect data and ensure compliance with regulatory standards. Financial institutions can leverage these security features, relieving the burden of maintaining and updating security protocols internally [9]. By entrusting the security of biometric data to reputable cloud providers, financial institutions can focus on core operations while benefiting from industry-leading security practices.

Common cloud-based biometric authentication techniques used in financial transactions

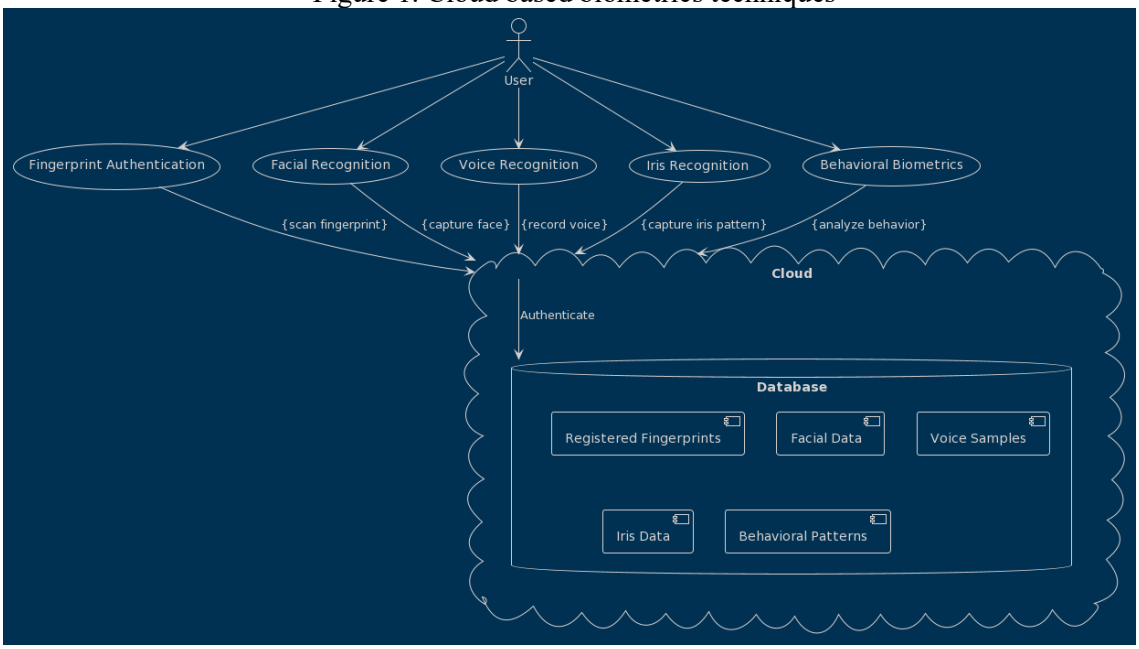
Cloud-based Fingerprint Authentication:

Cloud-based fingerprint authentication is a secure and efficient method of user authentication that utilizes cloud computing technology. The process involves capturing and scanning the user's fingerprint using a fingerprint scanner. The scanned fingerprint image is then transmitted to the cloud, where it is compared against a database of registered fingerprints [10]. This database, stored securely in the cloud, contains the biometric information of authorized users.

The cloud-based approach offers several advantages over traditional local storage of fingerprint data. Firstly, by storing the fingerprint database in the cloud, it becomes accessible from anywhere and at any time, provided there is an internet connection. This allows users to conveniently authenticate themselves on various devices, such as smartphones, tablets, or computers, without the need for local fingerprint storage. Additionally, cloud-based storage ensures that the fingerprint data is kept safe and secure, as cloud service providers typically employ robust security measures, such as encryption and access controls, to protect sensitive information [7].

The authentication process itself involves matching the scanned fingerprint against the registered fingerprints in the cloud database. This comparison is performed using sophisticated algorithms that analyze the unique characteristics of the fingerprint, such as ridge patterns and minutiae points [12]. By leveraging the processing power of cloud servers, the authentication process can be performed quickly and accurately, providing a seamless user experience. In the event of a match, the user is granted access to the desired application, system, or resource. Conversely, if there is no match, access is denied, ensuring the security and integrity of the protected resources.

Figure 1. Cloud based biometrics techniques



Cloud-based Facial Recognition:

Cloud-based facial recognition is an advanced biometric authentication method that utilizes cloud computing infrastructure to verify users' identities based on their facial features. The process involves capturing users' faces through a camera or webcam, and the facial image is then transmitted to the cloud for analysis. In the cloud, sophisticated facial recognition algorithms analyze various unique facial characteristics, such as the distance between the eyes, the shape of the nose, and the

arrangement of facial landmarks, to create a digital representation known as a facial template [12].

These facial templates are compared against a database of stored facial templates securely hosted in the cloud. This database contains the facial templates of registered users who have been previously enrolled in the system. The comparison process involves complex pattern matching and machine learning techniques to determine whether the captured facial image matches any of the stored templates. The cloud's computing power enables rapid processing of the facial recognition algorithms, resulting in a swift and accurate authentication process [13].

Since the facial data is stored in the cloud, users can perform facial authentication from virtually any device with a camera and internet connectivity, such as smartphones, tablets, laptops, or even specialized facial recognition terminals. This versatility makes cloud-based facial recognition suitable for various applications, including access control to physical locations, online identity verification, and secure authentication for mobile applications and services. Cloud service providers implement strong encryption and access controls to safeguard the facial templates stored in their servers, preventing unauthorized access and potential data breaches. Additionally, the cloud's scalability allows for the seamless addition of new users to the system, making it suitable for large-scale deployments and applications with dynamic user bases [14].

Cloud-based Voice Recognition:

The process begins by capturing the voice of the user through a microphone or any voice-enabled device. The captured voice sample is then transmitted to the cloud for analysis and authentication.

In the cloud, advanced voice recognition algorithms process the voice sample and extract distinctive characteristics, such as pitch, tone, cadence, and pronunciation. These features are used to create a unique voiceprint, also known as a voice template, that represents the individual's voice pattern. The voice template is securely stored in a cloud-based database, along with other pre-recorded voice samples of authorized users.

During the authentication process, the user's voice sample is compared against the stored voice templates in the cloud database. This comparison is performed using sophisticated pattern matching and machine learning algorithms. By analyzing the similarities and differences between the captured voice and the pre-recorded

samples, the system determines whether the voice matches any of the authorized users' templates [15].

Cloud-based voice recognition offers several benefits over traditional voice recognition systems. Firstly, the cloud infrastructure provides scalability and accessibility, allowing users to authenticate their voice from various devices and locations. This flexibility enables seamless integration of voice recognition into applications, devices, and services. Additionally, the cloud's computational power enables fast and accurate analysis of voice patterns, resulting in quick authentication responses.

Furthermore, cloud-based voice recognition offers enhanced security measures. Voice data is securely stored in the cloud using encryption and access control mechanisms to protect it from unauthorized access. The cloud's infrastructure also enables continuous monitoring and updates to ensure the system's security and integrity. This makes cloud-based voice recognition a reliable and secure authentication solution for a wide range of applications, including phone banking, voice assistants, and remote access systems [16].

Cloud-based Iris Recognition:

The process involves capturing high-resolution images of the user's irises using a specialized camera or iris scanner. These images are then transmitted to the cloud for analysis and authentication.

In the cloud, powerful iris recognition algorithms process the captured iris images and extract intricate and distinctive patterns such as the arrangement of crypts, furrows, and other unique features. These extracted patterns form a digital representation known as an iris template, which serves as a precise identifier for the individual's iris. The iris template is securely stored in a cloud-based database alongside other registered iris templates of authorized users [17].

During the authentication process, the user's captured iris images are compared against the stored iris templates in the cloud database. This comparison is carried out using advanced pattern recognition techniques, including template matching and statistical analysis. By measuring the level of similarity between the captured iris and the stored templates, the system determines whether the iris belongs to an authorized user or not.

Cloud-based iris recognition offers several advantages over traditional iris recognition systems. Firstly, the cloud-based approach allows for efficient and

scalable deployment of the technology across various applications and devices. Users can authenticate their irises from different locations and devices, making it a versatile solution for access control and identity verification. Moreover, the cloud's computational power enables fast and accurate analysis of iris patterns, resulting in rapid authentication responses. This is particularly crucial in scenarios where time-sensitive access control or identification is required. Additionally, the cloud infrastructure ensures that the iris data is securely stored and protected using encryption and access controls, minimizing the risk of unauthorized access to sensitive biometric information.

Cloud-based Behavioral Biometrics:

This approach focuses on capturing and analyzing various behavioral characteristics, such as typing speed, swipe gestures, or mouse movements, to establish a user's identity.

The process begins by collecting behavioral data from users as they interact with devices or applications. This data is then transmitted to the cloud for analysis and authentication. In the cloud, powerful machine learning algorithms process the behavioral data and extract relevant features that are unique to each individual [18].

Typing speed is one common behavioral pattern that can be analyzed. The way a user types, including factors like key press duration, key hold time, and the interval between keystrokes, can form a distinctive typing pattern. Similarly, swipe gestures or mouse movements, such as speed, acceleration, or trajectory, can be captured and analyzed to create a behavioral profile.

The cloud-based approach offers several advantages for behavioral biometrics. Firstly, it provides a flexible and scalable infrastructure, allowing the authentication process to be seamlessly integrated into various applications and platforms. Users can authenticate their identities from different devices or locations, making it a convenient solution for access control and identity verification [19].

Additionally, the cloud's computational power enables efficient analysis of large amounts of behavioral data, leading to accurate and reliable authentication results. Machine learning algorithms are employed to build models that can recognize and verify users based on their unique behavioral patterns. As more data is collected and analyzed in the cloud, these models can continuously learn and adapt to changes in users' behaviors, further enhancing the accuracy and security of the authentication process.

From a security perspective, cloud-based behavioral biometrics offers an additional layer of protection against identity theft and unauthorized access. Behavioral patterns are difficult to replicate, making it challenging for malicious actors to impersonate legitimate users. Furthermore, the cloud infrastructure ensures that the behavioral data is securely stored and transmitted, employing encryption and access controls to safeguard sensitive user information.

Process of Cloud-Based Biometric Authentication for Financial Transactions

Enrollment:

During the initial enrollment process, users are required to provide their biometric data to the system. This typically involves capturing biometric samples, such as fingerprints or facial features, through specialized devices such as fingerprint scanners or cameras. The captured biometric data is then securely transmitted and stored in the cloud [20].

To ensure the security and integrity of the biometric data, robust encryption techniques are employed during transmission and storage. This helps protect the data from unauthorized access or tampering. Cloud service providers implement stringent security measures, including access controls and multi-factor authentication, to safeguard the stored biometric data. These security measures are designed to meet industry standards and comply with privacy regulations to maintain user trust and confidentiality [21].

Authentication Request:

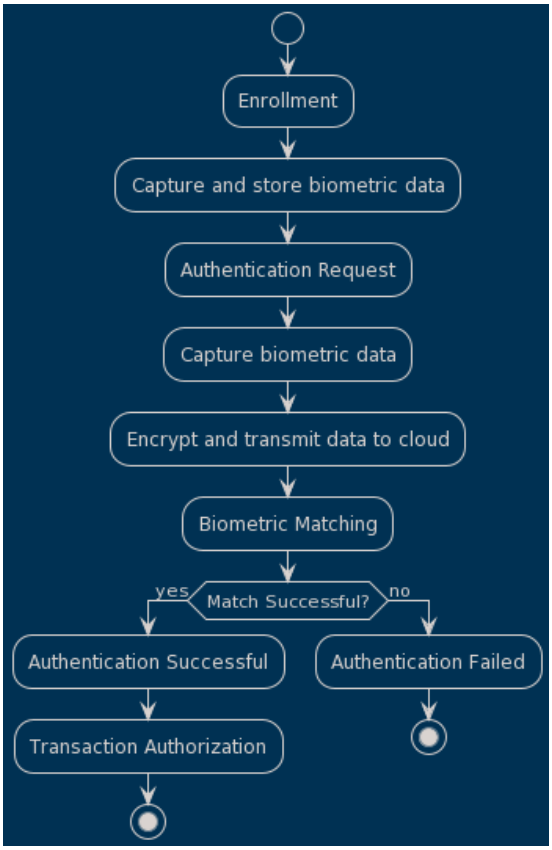
When users initiate a financial transaction, such as logging into a banking app or confirming a payment, they activate an authentication request that triggers the cloud-based authentication process. This request serves as a security measure to verify the user's identity and ensure the integrity of the financial transaction.

Upon receiving the authentication request, the cloud-based authentication system is prompted to initiate the verification process. The user's credentials, such as username or account information, are securely transmitted to the cloud server for validation. This initial step helps ensure that the user initiating the transaction is authorized to access the requested financial service.

Simultaneously, the cloud-based authentication system may also prompt the user to provide additional verification factors, depending on the security requirements of

the financial institution. These factors may include biometric data, such as fingerprints or facial recognition, or one-time passcodes sent to the user's registered mobile device or email address. The user's response or biometric data is captured and securely transmitted to the cloud for analysis and authentication.

Figure 2. Process of Cloud-Based Biometric Authentication for Financial Transactions



Biometric Data Capture:

To enable biometric authentication, the system utilizes the user's device equipped with appropriate sensors to capture the required biometric data, such as fingerprints or facial scans. This process allows for seamless and convenient authentication directly from the user's own device, whether it's a smartphone, tablet, or computer [22], [23].

When the authentication process is initiated, the device's built-in sensors, such as a fingerprint scanner or a front-facing camera, are activated to capture the biometric data [25]. For instance, in the case of fingerprint authentication, the user's finger is placed on the device's fingerprint scanner, which optically or capacitively captures the unique ridges and patterns on the fingertip. Similarly, in the case of facial recognition, the device's camera captures the user's facial features, including the arrangement of facial landmarks and the unique characteristics of the face.

Once the biometric data is captured by the device, it is securely processed and transmitted to the cloud for authentication. The captured data is typically encrypted to ensure its confidentiality during transmission. Cloud-based authentication systems use advanced algorithms and machine learning techniques to analyze and compare the captured biometric data with the stored biometric templates in the cloud. This comparison helps verify the user's identity and determine if the captured biometric data matches any of the enrolled biometric records [25].

By utilizing the user's own device and its integrated sensors, the authentication process becomes convenient and user-friendly. It eliminates the need for additional hardware or specialized authentication devices, as users can leverage the sensors already available on their devices. This approach also allows for a consistent and standardized user experience across different devices, ensuring compatibility and ease of use.

Data Transmission:

To ensure the security and integrity of the captured biometric data, it undergoes a series of protective measures before being transmitted to the cloud server for processing. Encryption techniques are applied to encrypt the data, rendering it unreadable to unauthorized parties during transmission.

When the biometric data is captured on the user's device, it is immediately encrypted using strong encryption algorithms. This process converts the biometric data into an encoded format that can only be deciphered with the corresponding decryption key.

Encryption helps safeguard the sensitive biometric information from interception or unauthorized access while it is in transit.

Once encrypted, the biometric data is securely transmitted over a network connection to the cloud server. This transmission is typically facilitated using secure communication protocols such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL). These protocols establish a secure and encrypted connection between the user's device and the cloud server, protecting the data from potential eavesdropping or tampering.

Upon arrival at the cloud server, the encrypted biometric data is received and stored in a secure manner. Cloud service providers employ robust security measures to protect the data, including access controls, firewalls, and intrusion detection systems. These measures are designed to prevent unauthorized access to the stored biometric data and ensure the privacy and confidentiality of the user's information.

When the cloud-based authentication system processes the biometric data, it utilizes the decryption key to decrypt the data and extract the relevant biometric features for analysis and comparison. This decryption process occurs within the secure cloud environment, where the data is safeguarded against potential security threats [26].

Biometric Matching:

In the cloud, the received biometric data undergoes a comparison process against the pre-registered data that was securely stored during the enrollment phase. This comparison step is crucial for authenticating the user's identity and determining if the captured biometric data matches any of the enrolled records.

Once the received biometric data is securely stored in the cloud, advanced matching algorithms and pattern recognition techniques are applied to analyze and compare the captured data with the stored pre-registered data. The cloud-based authentication system extracts relevant features and characteristics from both the received biometric data and the enrolled biometric templates [28].

For example, in the case of fingerprint authentication, the system analyzes the captured fingerprint minutiae, such as ridge endings and bifurcations, and compares them with the pre-registered fingerprint templates. Similarly, in the case of facial recognition, the system analyzes the captured facial features, such as the location of eyes, nose, and mouth, and compares them with the pre-registered facial templates.

During the comparison process, the system calculates a similarity score or a distance metric to determine the level of resemblance between the received biometric data and the enrolled data. This score indicates the degree of match between the captured biometric features and the stored templates.

Based on the comparison results, the system makes a decision regarding the authentication outcome. If the similarity score surpasses a predefined threshold, indicating a significant match, the user's identity is verified, and the authentication is deemed successful. Conversely, if the similarity score falls below the threshold, indicating a lack of sufficient match, the authentication is rejected.

Authentication Decision:

In the cloud-based biometric authentication system, the determination of whether the captured biometric data matches the enrolled data is made based on an appropriate confidence level. This confidence level represents the system's assessment of the similarity between the captured biometric features and the enrolled templates, providing a measure of certainty in the authentication process [28].

The system utilizes advanced algorithms and statistical methods to calculate the confidence level during the comparison between the captured biometric data and the enrolled data. These algorithms take into account various factors, such as the quality of the captured biometric sample, the complexity of the biometric pattern, and the variability of the enrolled templates.

During the comparison process, a similarity score or distance metric is computed, representing the degree of resemblance between the captured biometric data and the enrolled templates. The confidence level is derived from this score, with higher scores indicating a stronger match and therefore a higher level of confidence in the authentication result [29].

The appropriate confidence level is determined based on the specific requirements and security policies of the application or system using the biometric authentication. These requirements may vary depending on the sensitivity of the data or the criticality of the operation being performed. For highly secure applications, a higher confidence level may be set, requiring a closer match between the captured and enrolled biometric data to authenticate the user's identity.

The confidence level threshold is typically defined and set by the system administrator or the organization implementing the biometric authentication system.

It is chosen to balance between security and user convenience, ensuring that the authentication process is reliable while avoiding excessive false rejection rates.

Transaction Authorization:

Upon successful authentication, granting a positive match between the captured biometric data and the enrolled data, the cloud-based biometric authentication system authorizes the financial transaction, enabling the user to proceed with the desired action. This authorization signifies that the user's identity has been verified and validated, providing them with access to perform sensitive operations or access restricted information.

For instance, if the user is initiating a money transfer, the successful authentication ensures that the user is the authorized account holder, thereby allowing them to proceed with the transaction securely. Similarly, if the user is attempting to access sensitive information or perform a high-level operation within a financial application, the successful authentication grants them the necessary authorization to proceed.

The authorization process is typically performed in conjunction with the financial application or service that requested the authentication. Once the cloud-based biometric authentication system confirms the user's identity, it sends a verification signal back to the financial application, indicating that the authentication was successful. This signal serves as a trigger to allow the desired action to take place, as it confirms that the user has been verified and can proceed securely [30].

By authorizing the financial transaction or granting access to sensitive information, the cloud-based biometric authentication system ensures that only authorized individuals can perform such operations [31]. This helps prevent unauthorized access, fraud, or misuse of financial resources, providing an additional layer of security and confidence to the user and the financial service provider.

Conclusion

The adoption of cloud computing for biometrics authentication in financial institutions brings numerous advantages, including secure storage and processing of biometric data, scalability to meet fluctuating demand, and enhanced security through leveraging the expertise of cloud service providers. The combination of cloud computing and biometric authentication empowers financial institutions to provide robust security measures, seamless user experiences, and cost-effective solutions, ensuring the integrity of customer identities and safeguarding against fraudulent activities in the ever-evolving digital landscape.

Biometric authentication offers an advanced level of security by leveraging unique biological traits that are difficult to replicate or forge. Unlike traditional authentication methods like passwords or PINs, which can be easily stolen, forgotten, or hacked, biometric traits such as fingerprints, iris patterns, or facial features are highly individualized and extremely difficult to duplicate. This adds a robust layer of security, as unauthorized individuals would need physical access to the biometric data to attempt any fraudulent activity. Biometric authentication systems also employ sophisticated algorithms to analyze and match biometric data, ensuring that only authorized users with valid biometric traits can gain access to sensitive information or secure physical locations. With enhanced security provided by biometric authentication, organizations can better protect their digital assets and confidential data from unauthorized access and potential cyber threats.

Biometric authentication eliminates the need for users to remember and manage multiple passwords or PINs, which are often associated with common inconveniences such as forgotten credentials or frequent password resets. With biometrics, users can simply present their unique physiological or behavioral traits for authentication, streamlining the authentication process and enhancing user convenience. Users no longer need to rely on their memory or carry around physical tokens like access cards or keys. Biometric traits are inherently attached to individuals, making authentication a seamless and user-friendly experience. Moreover, biometric authentication can be integrated into various devices and applications, such as smartphones, laptops, or even payment systems, providing a consistent and unified authentication experience across different platforms. This convenience factor not only enhances user experience but also improves productivity by reducing time wasted on password-related issues.

Cloud-based biometric authentication systems play a significant role in reducing the risk of identity theft and fraudulent transactions. By utilizing biometric traits as the primary authentication factor, organizations can establish a more robust and reliable identity verification process. Biometric traits, such as fingerprints or facial scans, are unique to each individual and cannot be easily duplicated, making it significantly harder for malicious actors to impersonate authorized users. This helps prevent fraudulent activities, such as unauthorized access to user accounts, financial fraud, or fraudulent transactions. Furthermore, cloud-based biometric authentication systems leverage advanced encryption techniques and secure communication channels to transmit and store biometric data, ensuring its integrity and confidentiality. By reducing the risk of identity theft and fraud, organizations can enhance trust and confidence among their customers, ultimately safeguarding their reputation and fostering long-term relationships with users.

One of the most concerning issue in cloud-based biometrics is the reliance on cloud computing introduces a single point of failure. If the cloud server experiences downtime or faces cyberattacks, financial transactions relying on cloud-based biometric authentication could grind to a halt. This vulnerability highlights the need for robust backup and redundancy measures to ensure continuous service availability.

References

[1] Q. Xiao, "Security issues in biometric authentication," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, 2005, pp. 8–13.

[2] P. Ambalakat, "Security of biometric authentication systems," *21st Computer Science Seminar*, 2005.

[3] S. Venkatraman and I. Delpachitra, "Biometrics in banking security: a case study," *Inf. Manage. Comput. Secur.*, vol. 16, no. 4, pp. 415–430, Jan. 2008.

[4] R. C. Agidi, "Biometrics: the future of banking and financial service industry in Nigeria," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 91–105, 2018.

[5] S. Ghosh, "Financial inclusion, biometric identification and mobile: unlocking the JAM trinity," *International Journal of Development Issues*, vol. 16, no. 2, pp. 190–213, Jan. 2017.

[6] S. M. Matyas and J. Stapleton, "A Biometric Standard for Information Management and Security," *Comput. Secur.*, vol. 19, no. 5, pp. 428–441, Jul. 2000.

[7] A. Fatima, "E-banking security issues – is there A solution in biometrics?," *Journal of internet banking and commerce*, 2011.

[8] S. Z. Li and A. K. Jain, *Encyclopedia of Biometrics: I - Z*. Berlin, Germany: Springer, 2009.

[9] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," *Symmetry* , vol. 11, no. 2, p. 141, Jan. 2019.

[10] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, "Provably secure biometric-based user authentication and key agreement scheme in cloud computing," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4103–4119, Nov. 2016.

[11] A. S. Bommagani, M. C. Valenti, and A. Ross, "A Framework for Secure Cloud-Empowered Mobile Biometrics," in *2014 IEEE Military Communications Conference*, 2014, pp. 255–261.

[12] T. Bhattasali, K. Saeed, N. Chaki, and R. Chaki, "A Survey of Security and Privacy Issues for Biometrics Based Remote Authentication in Cloud," in

Computer Information Systems and Industrial Management, 2014, pp. 112–121.

[13] H.-H. Zhu, Q.-H. He, H.-H. Zhu, H. Tang, and W.-H. Cao, "Voiceprint-biometric template design and authentication based on cloud computing security," in *2011 International Conference on Cloud and Service Computing*, 2011, pp. 302–308.

[14] J. Ashbourn, *Biometrics in the new world: The cloud, mobile technology and pervasive identity*. New York, NY: Springer, 2014.

[15] M. N. Omar, M. Salleh, and M. Bakhtiari, "Biometric encryption to enhance confidentiality in Cloud computing," in *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*, 2014, pp. 45–50.

[16] C. Hahn and J. Hur, "Efficient and privacy-preserving biometric identification in cloud," *ICT Express*, vol. 2, no. 3, pp. 135–139, Sep. 2016.

[17] F. Omri, R. Hamila, S. Foufou, and M. Jarraya, "Cloud-Ready Biometric System for Mobile Security Access," in *Networked Digital Technologies*, 2012, pp. 192–200.

[18] I. A. L. Rassan and H. AlShaher, "Securing Mobile Cloud Computing Using Biometric Authentication (SMCBA)," in *2014 International Conference on Computational Science and Computational Intelligence*, 2014, vol. 1, pp. 157–161.

[19] P. Peer, Ž. Emeršič, J. Bule, J. Žganec-Gros, and V. Štruc, "Strategies for Exploiting Independent Cloud Implementations of Biometric Experts in Multibiometric Scenarios," *Math. Probl. Eng.*, vol. 2014, Mar. 2014.

[20] M. Stojmenovic, "Mobile Cloud Computing for Biometric Applications," in *2012 15th International Conference on Network-Based Information Systems*, 2012, pp. 654–659.

[21] G. L. Masala, P. Ruiu, and E. Grosso, "Biometric Authentication and Data Security in Cloud Computing," in *Computer and Network Security Essentials*, K. Daimi, Ed. Cham: Springer International Publishing, 2018, pp. 337–353.

[22] D. Shah and V. Haradi, "IoT Based Biometrics Implementation on Raspberry Pi," *Procedia Comput. Sci.*, vol. 79, pp. 328–336, Jan. 2016.

[23] P. Rajeswari, S. Viswanadha Raju, A. S. Ashour, and N. Dey, "Multi-fingerprint Unimodel-based Biometric Authentication Supporting Cloud Computing," in *Intelligent Techniques in Signal Processing for Multimedia Security*, N. Dey and V. Santhi, Eds. Cham: Springer International Publishing, 2017, pp. 469–485.

[24] E. Kohlwey, A. Sussman, J. Trost, and A. Maurer, "Leveraging the Cloud for Big Data Biometrics: Meeting the Performance Requirements of the Next

Generation Biometric Systems," in *2011 IEEE World Congress on Services*, 2011, pp. 597–601.

[25] Z. Wu, L. Tian, P. Li, T. Wu, M. Jiang, and C. Wu, "Generating stable biometric keys for flexible cloud computing authentication using finger vein," *Inf. Sci.* , vol. 433–434, pp. 431–447, Apr. 2018.

[26] B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Towards secure cloud-centric Internet of Biometric Things," in *2015 IEEE 4th International Conference on Cloud Networking (CloudNet)*, 2015, pp. 81–83.

[27] C. Zhang, L. Zhu, and C. Xu, "PTBI: An efficient privacy-preserving biometric identification based on perturbed term in the cloud," *Inf. Sci.* , vol. 409–410, pp. 56–67, Oct. 2017.

[28] S. Kumar, S. K. Singh, A. K. Singh, S. Tiwari, and R. S. Singh, "Privacy preserving security using biometrics in cloud computing," *Multimed. Tools Appl.*, vol. 77, no. 9, pp. 11017–11039, May 2018.

[29] V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," *Multiscale and Multidisciplinary Modeling, Experiments and Design*, vol. 2, no. 4, pp. 233–248, Dec. 2019.

[30] L. Zhu, C. Zhang, C. Xu, X. Liu, and C. Huang, "An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing," *IEEE Access*, vol. 6, pp. 19025–19033, 2018.

[31] P. Padma and S. Srinivasan, "A survey on biometric based authentication in cloud computing," in *2016 International Conference on Inventive Computation Technologies (ICICT)*, 2016, vol. 1, pp. 1–5.