Research Article – Vol. 03, Issue 01, No. 06

Advanced in Engineering and Intelligence Systems

Journal Web Page: https://aeis.bilijipub.com

Biometric Fusion for Enhanced Authentication in Cloud Computing Environments

Chiyo Miyazawa[1], Ryosuke Sato[2, *]

[1] Osaka Univ, Grad Sch Engn, Div Elect Elect & Infocommun Engn, Suita, Osaka 5650871, Japan
[2] NTT Corp, NTT Device Technol Labs, Atsugi, Kanagawa 2430198, Japan

Highlights

- Introduction of MultiFusionGuard, a multimodal biometric authentication framework for cloud security.
- Utilizes diverse biometric traits like fingerprints, iris scans, and palm prints for enhanced security.
- Meticulous image processing stages including pre-processing, normalization, and feature extraction.
- Fusion of multiple biometric features at various levels for a robust authentication system, evaluated for reliability and resilience.

Article Info

Received: 13 February 2024
Received in revised: 25 March 2024
Accepted: 30 March 2024
Available online: 30 March 2024

Keywords

Cloud security
Multimodal biometrics
Authentication
Cryptographic
Data protection
Biometric fusion

Abstract

In the realm of cloud computing, ensuring robust data security is of utmost importance. Authentication, a cornerstone of safeguarding information, continuously evolves to counter escalating threats. This paper introduces MultiFusionGuard, an innovative multimodal biometric authentication framework aimed at bolstering cloud security. By leveraging diverse biometric traits like fingerprints, iris scans, and palm prints, MultiFusionGuard utilizes their unique patterns to enhance security measures. Each trait undergoes meticulous image processing stages, encompassing pre-processing, normalization, and feature extraction. The fusion of these distinct biometric features at multiple levels results in a robust authentication framework. Integration of these features establishes a comprehensive and intricate authentication system, thereby amplifying the complexity and effectiveness of security measures. The system's efficacy is evaluated using indicators such as incorrect rejection ratio, incorrect acceptance ratio, and execution time to ensure reliability and resilience against illegal access attempts. MultiFusionGuard offers a promising solution to fortify data protection within cloud environments, providing advanced defense mechanisms against potential security breaches.

1. Introduction

Cloud Computing has emerged as a pivotal advancement in network technology in recent years. The fundamental concept behind cloud computing revolves around furnishing pertinent services by distributing hardware resources and software applications under users' specific requirement[1]. Within the realm of cloud computing architecture, there exist three distinct classifications, with Software as a Service (SaaS) being the initial type. Within the SaaS framework, the system proffers software resources accessible via the platform, simplifying user interaction. The second classification is Platform as a Service (PaaS), which facilitates users in creating and developing their projects through the platform. The final classification is Infrastructure as a Service (IaaS). This category enables users to store, execute, and undertake computational operations without procuring hardware devices[2], [3].

Cloud computing encompasses four distinct deployment models, elucidated in Fig. 1: private, public,

[*] Corresponding Author: Ryosuke Sato
Email: Ryosukesato776@gmail.com

community, and hybrid clouds. Private clouds entail utilizing cloud services within or outside an organization's premises, residing within the firewall of a virtualized data center. Service provision in this model is limited to infrastructure by cloud service providers, precluding user control over services. On the other hand, public clouds cater to the needs of the general public or large industries, being owned and dispensed by cloud service organizations. Within public clouds, the infrastructure and service control are managed solely by the cloud service providers outside the firewall in a virtualized data center. Accessible over the Internet on an on-demand basis, these services serve the public at large. Meanwhile, community clouds involve the sharing of cloud services among multiple organizations that share common concerns or interests. Lastly, hybrid clouds represent a fusion of two or more cloud models, unified through standardized or proprietary technology facilitating the portability of data and applications[4].

Within the domain of the cloud environment, numerous security threats necessitate attention, specifically concerning data confidentiality, integrity assurance, robustness, authorization, and the establishment of accountability between cloud service providers and consumers[5]. User access management in cloud computing demands meticulous attention, requiring appropriate certification, licensing, and quarantine protocols to thwart potential threats such as hackers, viruses, and other vulnerabilities. The issue of data privacy assumes heightened significance compared to traditional networks. Key privacy concerns encompass inadequate authentication, authorization, deficient account controllability, and suboptimal key management practices. Among the array of potential threats in the cloud computing milieu, Distributed Denial of Service (DDoS) attacks pose a significant risk, their impact amplified due to multiple resource sharing. While augmenting resources traditionally can mitigate such attacks, malicious actors deliberately target these systems through botnets. Intrusion Prevention Systems (IPS) offer a potential avenue for effective mitigation against DDoS attacks; however, akin to firewalls, they remain susceptible. Addressing DDoS concerns necessitates a dedicated focus on network layer virtualization[6].

Within multitenancy frameworks, resources are distributed among numerous tenants, enabling the sharing of common logical addresses, storage space, and applications. However, tenants operate within an environment where the internal flow of data or processes remains concealed. Ensuring transparency in this flow becomes imperative for tenants, alongside the crucial requirement of isolating data across different services[7]. Addressing the challenges arising from multitenancy involves various strategies: isolating data through the separation of virtual machines (VMs) in IaaS, achieving data isolation through the segregation of application programming interface (API) services and operating systems in PaaS, and obtaining segregated data by concurrently running transactions separately for different tenants in SaaS. In elastic cloud computing environments, clients can adjust their resource requirements on an on-demand basis, scaling up or down as needed. However, transferring resources from one customer to another poses a potential risk to data confidentiality. The allocation of resources from the service placement engine must diligently uphold the security and legal requirements of the cloud's consumers to mitigate such risks effectively[8].

The primary security concern in cloud computing revolves around privileged user access, given that external organizations handle the data, necessitating stringent access privileges to prevent both physical and logical data loss. In cloud environments, restricting access solely to authorized users for account management inadvertently opens avenues for unauthorized access to the management interface[9]. A notable challenge in cloud environments is data recovery following sudden data loss. Moreover, reallocating user resources at different intervals introduces the possibility of a new user retrieving data from previously allocated resources, thereby raising concerns about data exposure. Resource allocation dynamics within the cloud, driven by pooling and elasticity characteristics, underscore the need to address these vulnerabilities. Addressing internet protocol vulnerabilities is critical for cloud security. Performance impediments stemming from internet protocol vulnerabilities, such as man-in-the-middle attacks and IP spoofing, emerge due to the reliance of cloud services on the internet. Clouds encounter issues related to metering and billing evasion.

Since metering is crucial for appropriate service provision in cloud environments due to inherent measuring traits, tampering can impact service delivery and billing accuracy. Additionally, there's a pressing need to counter malware injection attacks in the cloud, where malicious software, applications, or virtual machines are crafted by hackers and inserted into the cloud infrastructure, disrupting regular program execution and potentially leading to unauthorized access, data theft, and eavesdropping. Ensuring regulatory compliance demands external audits in cloud services. Providing details concerning data location or movement to users becomes crucial for bolstering data segregation security, considering its shared nature and the imperative of maintaining long-term viability. While encryption and decryption keys are conventional measures to secure data transmission, their application in handling larger volumes of data and users within the cloud context can become cumbersome and time-consuming[10].

Authentication in cloud computing is a critical aspect of ensuring data security and integrity. Traditional methods often rely on complex cryptographic algorithms, but with the evolution of technology, these methods are increasingly vulnerable to sophisticated attacks. As such, there's a growing need for more robust authentication systems. Biometrics presents a promising solution, leveraging unique biological traits such as fingerprints, iris patterns, and palm prints for user verification. Unlike traditional methods, biometric authentication offers a higher level of individuality and security. However, to further enhance authentication in the cloud, adopting multimodal biometric systems like MultiFusionGuard is imperative. MultiFusionGuard goes beyond single biometric traits by fusing multiple modalities, thereby strengthening the authentication process. By harnessing diverse biometric features at multiple levels, MultiFusionGuard establishes a comprehensive and intricate authentication framework, augmenting the complexity and strength of security measures in cloud environments. This innovative approach promises to fortify data protection and mitigate various security threats, providing an advanced and formidable defense against potential breaches.

Cryptography, or cryptology, revolves around converting human-readable information into an unreadable format, a process termed encryption. Decryption refers to the reverse mechanism of this process. Common cryptographic algorithms include symmetric key cryptography (SKC), asymmetric key cryptography (AKC), and hash functions. In SKC, a shared secret key encrypts and decrypts messages; anyone possessing the secret key can read the message. Conversely, AKC employs two keys, the public and private keys, in the encryption process. The public key is disseminated widely, while the private key remains confidential. The validity of both keys enables message decryption. Hashing, employed when transforming a message into an irretrievable collection of characters or numbers, represents a "one-way encryption", rendering the original message irretrievable.

The research contributions of this study are as,

1.The study introduces a method of leveraging multiple biometric modalities, including palm print, iris, and fingerprint attributes, to enhance authentication in cloud environments. By combining these unique biological patterns, the system generates a confidential key, which is crucial for secure data transmission and storage.

2. The research incorporates cryptographic algorithms such as Blowfish, AES, and DES to encode and protect data using the generated confidential key. These algorithms ensure data confidentiality and integrity, enhancing security measures within the cloud environment.

3. By combining multiple biometric modalities and cryptographic algorithms, the study significantly improves authentication mechanisms and data security in cloud computing. This enhancement is vital for addressing concerns regarding data confidentiality, integrity, and unauthorized access, ultimately bolstering the overall security posture of cloud-based collaborative software services.

The structure of this paper is delineated as follows: Section 2 delves into related work in the field. Section 3 comprehensively articulates the workflow of the proposed model. In Section 4, the results derived from this research are presented, and their significance is discussed. Finally, Section 5 encapsulates the work by emphasizing the findings and conclusions drawn.

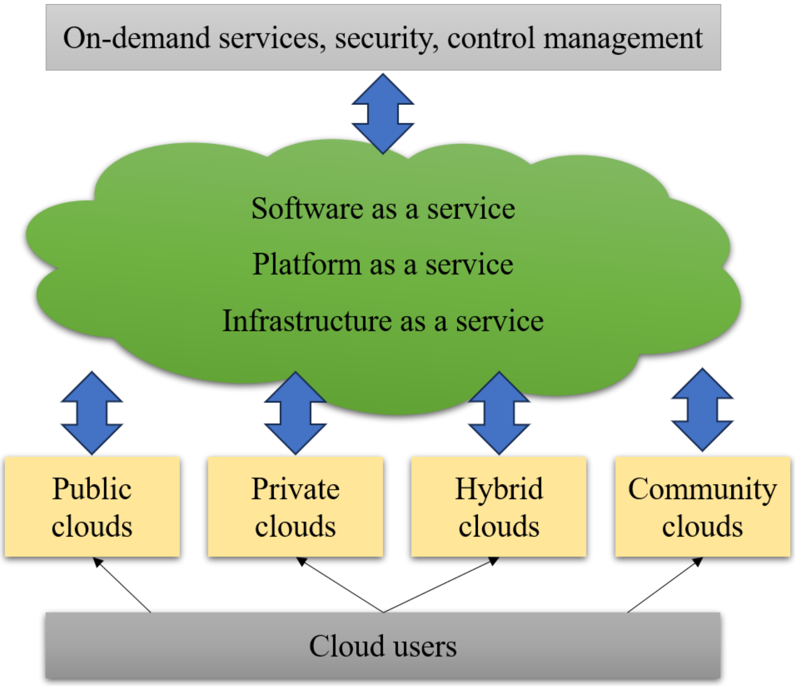

Fig. 1. General cloud computing model

2. Related works

The advent of cloud computing has fundamentally transformed the data storage, transmission, and computation domain. User authentication is the primary security measure at the outset of cloud computing. Nevertheless, conventional authentication systems that rely on biometric templates have difficulties arising from the possible disclosure of biometric template data and the restrictions imposed by users' capacity to remember keys. Table 1 summarizes the key focuses, methodologies used, and main contributions of prior studies dealing with security concerns in cloud computing and authentication techniques.

Wu, et al. [11] presented the FVHS algorithm as a new method for generating bio-keys. This methodology combines the advantages of biometric and user-key authentication. FVHS generates durable and adequately resilient bio-key sequences from finger vein biometrics. A novel framework called FVHS is introduced for cloud computing authentication, which provides improved flexibility, ease, and security in user authentication. The fundamental idea behind FVHS is integrating machine learning, biometrics, and cryptography to derive a unique feature vector from the biometric domain. Subsequently, this vector transforms and is rendered stable, resulting in a fixed numerical sequence within a space of greater dimensions. The effectiveness of FVHS in obtaining reliable biometric features from high-quality finger vein pictures is supported by theoretical analysis and experimental confirmation. FVHS attains a Genuine Accept Rate of 99.9%, a False Accept Rate below 0.8%, and an Equal Error Rate of less than 0.5%. Furthermore, it guarantees a security level of 256 bits.

Sarier [12] developed a novel Privacy-Preserving Biometric Authentication (PPBA) system specifically designed for Mobile Edge Computing (MEC) and multimodal biometrics. Their primary objective is to mitigate hill-climbing attacks that involve the exposure of encrypted biometric templates to insider adversaries, even when these templates are stored in the cloud. At first, they provide a scenario where it is impossible to have two-party PPBA systems that can withstand these attacks. To tackle this difficulty, they propose the implementation of a non-colluding edge server specifically built to identify hill-climbing assaults in both semi-honest and malicious scenarios. The edge server stores the private parameters of each user and allows for the transfer of the biometric database to the cloud. It also performs matching operations within the encrypted domain. The suggested approach combines Set Overlap and Euclidean Distance metrics at the score level. Significantly, neither the cloud nor the edge servers can infer the combined matching score. In addition, strict precautions prohibit the edge server from accessing any incomplete score. The efficiency of the cryptographic primitives used for each biometric modality leads to a direct increase in computing and communication overhead. An assessment conducted under several MEC scenarios demonstrates that the new system achieves maximum efficiency with a 2-tier design, resulting in a 75% decrease in latency compared to mobile cloud computing.

Gumaei, et al. [13] have proposed an innovative solution to overcome the constraints commonly seen in cloud-based biometric identification systems and methodologies. The limitations encompass concerns such as data with high noise levels, variances within and between classes, significant time expenses, errors, lack of universality, and susceptibility to spoofing attacks. In response to these problems, they have suggested an anti-spoofing multi-spectral biometric method for cloud-based identification, focusing on safeguarding privacy and enhancing security in cloud computing environments. Their methodology focuses on utilizing multi-spectral palmprint data as a representative biometric characteristic and consists of two main stages: an offline enrollment stage and an online identification stage. This work is the first effort to protect privacy in cloud computing by utilizing encrypted multi-spectral palmprint features. This approach effectively eliminates any risks of information leakage or disclosure issues. The experimental results demonstrated the efficacy of their method in effectively and efficiently safeguarding the confidentiality and integrity of data stored in the cloud.

Singh and Natarajan [14] developed a robust authentication mechanism specifically designed for digitizing personal health records within a user's domain. This protocol uses a cryptographic key during data exchanges to guarantee confidentiality and integrity. In contrast to numerous current protocols that depend on elliptic curve cryptography, their suggested protocol adopts a distinctive method. At first, it utilizes the Kyber cryptographic algorithm, which is both asymmetric and resistant to quantum attacks, during the initial phases. It then employs the Advanced Encryption Standard in Galois/Counter mode (AES-GCM), a symmetric cryptographic technique, to ensure the security of the sent data. A notable feature of this protocol is its approach to ensuring transaction security without directly exchanging the actual key. Moreover, the protocol serves the purpose of confirming the user's identity and ensuring their legitimate citizenship. The system utilizes a session-based methodology, creating a fresh key for each session to guarantee secure transactions. The protocol was subjected to a thorough study of multiple security aspects with the ProVerif tool. The findings demonstrated substantial enhancements in security measures, decreased expenses for storage, and improved computational effectiveness compared to similar protocols within the field.

Singh, et al. [15] have developed an efficient encryption and verification system specifically tailored to cloud-based IoT applications. This system utilizes elliptic curve cryptography to guarantee complete anonymity. Their proposed mechanism addresses multiple essential security aspects, namely availability, forward secrecy, integrity, privacy, user anonymity, co-authentication, and key generation. A comprehensive security analysis was conducted, which verified that the proposed mechanism is resilient against a wide range of potential attacks, including replay attacks, user and gateway impersonation, denial of service attacks, man-in-the-middle attacks, lost or stolen device scenarios, de-synchronization issues, known-key attacks, parallel session attacks, gateway bypassing attempts, and offline password guessing. Security assessments were performed utilizing BAN logic and the ROR model to improve its security capabilities.

Shukla and Patel [16] have developed a cutting-edge authentication mechanism tailored for the cloud environment. This protocol utilizes elliptic curve cryptography (ECC) to guarantee security and anonymity. This protocol offers robust user anonymity, unlinkability, perfect forward secrecy, and session key security as its primary authentication characteristics. The protocol's theoretical security has been thoroughly established using the Real-Or-Random (ROR) model. The protocol was verified using the Scyther security verification tool to confirm its correctness properties. During an informal security examination, the protocol demonstrated robustness against multiple security threats, including replay attacks, Denial of Service (DoS) assaults, Key-Server Side-Channel Timing Attacks (KSSTI), user impersonation, server spoofing, password-guessing, and privileged insider attacks. Furthermore, a comprehensive examination was conducted to compare the existing protocols, assessing their security features, communication methods, and computing burdens. The results indicate that the suggested protocol provides enhanced security while keeping communication and computational costs at an acceptable level compared to similar protocols currently in use.

Santos, et al. [17] have implemented a system to resolve the significant issues related to data security in cloud computing. The extensive implementation of cloud computing has faced obstacles arising from ambiguous safeguards developing regulations concerning data protection and privacy practices. An essential focus is to guarantee strong data security while preserving the authenticity of user identities and protecting the virtual environment from possible breaches. Their suggested approach addresses the issue of unwanted access to data stored in public clouds by utilizing a fragmentation technique in conjunction with a NoSQL database. The objective of this strategy is to mitigate unlawful entry and bolster the security of data. Moreover, the system incorporates a mechanism for overseeing and verifying users through multimodal biometrics, guaranteeing strong user authentication. Significantly, safeguards are implemented to safeguard the biometric characteristics from security breaches. The proposed fragmentation methodology demonstrates superior latency performance when compared to encryption methods. This feature makes it a desirable solution, particularly in areas with strict latency demands, such as healthcare IT infrastructure, indicating its significant potential in practical situations.

Table 1. Comparison of security-enhancing based techniques in cloud computing

Reference	Key focus	Methodology	Main contributions
[11]	Bio-key generation combining biometrics and user-key authentication	Integration of machine learning, biometrics, and cryptography for bio-key generation	It achieves a high genuine accept rate and a low false accept rate
[12]	Privacy-preserving biometric authentication; Mitigating hill-climbing attacks; Mobile edge computing	Utilization of a non-colluding edge server for identifying hill climbing assaults in MEC scenarios	The proposed system mitigates hill-climbing attacks in semi-honest and malicious scenarios, decreases latency by 75% in MEC scenarios
[13]	Anti-spoofing multi-spectral palmprint biometrics for cloud-based identification; Privacy-focused methodology	Use of encrypted multi-spectral palmprint features for privacy in cloud computing	Methodology protects privacy using encrypted multi-spectral palmprint features and ensures data confidentiality and integrity in the cloud.
[14]	Robust authentication mechanism for digitizing personal health records; Use of Kyber cryptographic algorithm and AES-GCM	Utilization of Kyber cryptographic algorithm and AES-GCM for secure data exchange	Secure protocol using Kyber cryptographic algorithm and AES-GCM; Improved security, reduced storage costs, enhanced computational efficiency
[15]	Authentication and key agreement system for cloud-based IoT applications; Focus on anonymity and various security aspects	Utilization of elliptic curve cryptography for complete anonymity in cloud-based IoT applications	Enhanced security with resistance against multiple attacks; Elimination of secure channel for registering IoT nodes with the gateway
[16]	Cloud authentication protocol focusing on elliptic curve cryptography; Emphasis on security and anonymity.	Usage of elliptic curve cryptography for user anonymity and perfect forward secrecy	Robust authentication with security against various attacks: Anonymity, unlinkability, perfect forward secrecy, and session key security
[17]	Data security in cloud computing via fragmentation and multimodal biometrics; Focus on latency performance and user authentication	Fragmentation technique with NoSQL database for data security; Multimodal biometrics for authentication	Improved data security with fragmentation; Latency performance advantage; Strong user authentication and identity verification

3. Proposed system

The fundamental biometric trait utilized for authentication is the fingerprint, which is known for its uniqueness. However, fingerprint images captured from sensors may contain noise or occlusions. Specific pre-processing techniques are applied to the image data to mitigate these issues. The following steps are executed to extract the feature region from the input fingerprint data:

- Image normalization and segmentation: The grayscale image undergoes adjustments within a specified value range to standardize the image's intensity.
- Orientation estimation: Initial computation of gradients is performed for each pixel within the image. Subsequently, local orientation is determined by identifying the variation axis in the image gradients. The orientation field is then smoothed using the Gaussian low-pass filter method.
- Morphological processing: Preceding the extraction of minutiae points from the fingerprint, an image thinning process is conducted, emphasizing the ridges and establishing a mapping of feature points. This step results in generating a skeletal pattern of ridges.

- Extraction of the region of interest (ROI): Feature points are derived from the skeletal image utilizing two morphological operations, namely ERODE and OPEN.

The framework of the multimodal biometric authentication system is illustrated in Fig 2, demonstrating the outlined processes. Moreover, Fig 3.a depicts the method used for fingerprint feature point extraction. The iris, an integral part of the human eye, exhibits unique structural patterns distinctive to each individual, making it a robust method for user authentication in highly secure processes. Various successful approaches have been developed to extract the iris's region of interest. In this system, several methods are employed, outlined below. Fig 3.b illustrates the iris feature point extraction method. Initially, the iris image data undergoes binarization using the Otsu thresholding technique. Next, the Canny edge detection method is employed to trace the curvature of the image's edges. The Hough transform is used to identify the limits of the edge-detected image. Ultimately, the Gabor filtering technique is employed to retrieve distinct characteristics pertaining to the iris region.

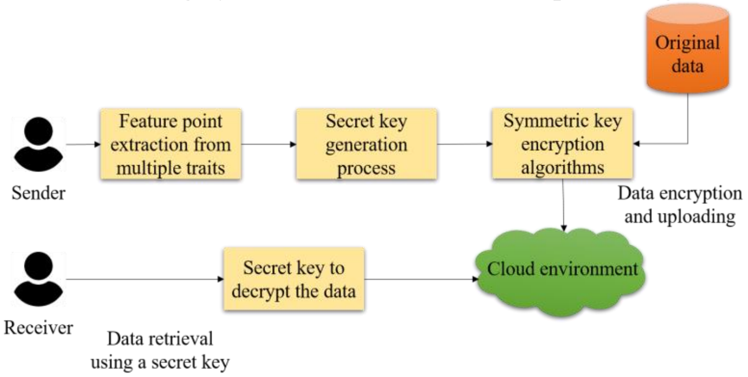
Original data
Sender
Feature point extraction from multiple traits
Secret key generation process
Symmetric key encryption algorithms
Data encryption and uploading
Cloud environment
Receiver
Secret key to decrypt the data
Data retrieval using a secret key

Fig. 2. Multimodal biometric authentication system

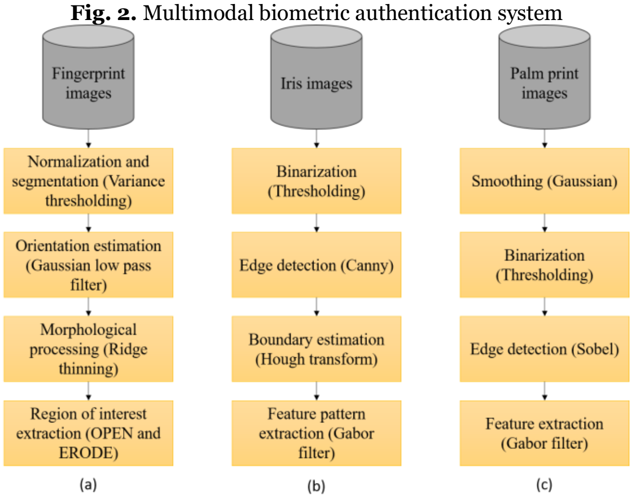
Fingerprint images
Normalization and segmentation (Variance thresholding)
Orientation estimation (Gaussian low pass filter)
Morphological processing (Ridge thinning)
Region of interest extraction (OPEN and ERODE)
(a)
Iris images
Binarization (Thresholding)
Edge detection (Canny)
Boundary estimation (Hough transform)
Feature pattern extraction (Gabor filter)
(b)
Palm print images
Smoothing (Gaussian)
Binarization (Thresholding)
Edge detection (Sobel)
Feature extraction (Gabor filter)
(c)

Fig. 3. Multimodal biometric authentication system

The process of identifying and monitoring the palm area on hands is complicated by factors such as noise, variations within the same class, and the presence of delicate ridges. Although there are other challenges involved, utilizing the palm area for authentication guarantees the integrity of the authentication system because of its intrinsic uniqueness. The procedure for extracting this characteristic entails the subsequent stages, as depicted in Fig 3.c, which illustrates the method for extracting feature points from palm prints.

- Smoothing: The collected picture from the sensor is initially subjected to Gaussian smoothing to minimize noise and improve clarity.
- Binarization: Afterwards, the smoothed image is converted into a binary form using the Otsu thresholding method.
- Region detection: The Sobel edge detection method is utilized on the binarized data to find palm regions, facilitating the demarcation of palm boundaries.
- Feature extraction: The 2D-Gabor Wavelet approach is used to extract feature points from the specified palm zone.

After extracting the feature points from each trait, they are transformed into a binary pattern. Each pixel's value in the identified features is thresholded and replaced by either

0 or 1, generating a sequence of binary values comprising the final feature vector. The XOR module functions in a dual-phase manner to combine the three binary values derived from each feature. During stage 1, the fingerprint and iris feature vectors are merged using XOR operations, resulting in the creation of a novel vector. Subsequently, the obtained value is subjected to another XOR operation with the binary representation of the third characteristic, namely the palm print. The output of this process yields a unique binary key. Fig 4 depicts the process of generating secret keys using the multimodal biometric mechanism.

The MD-5 algorithm, also known as the message-digest algorithm, is a commonly used method for hashing that generates a 265-bit key. Its main purpose is to guarantee the reliability of authentication procedures, like password protection. The resulting XOR array of features is ultimately converted into a 128-bit hash string via MD-5. The hash key serves as the paramount confidential key for encrypting and decrypting data in a cloud context.

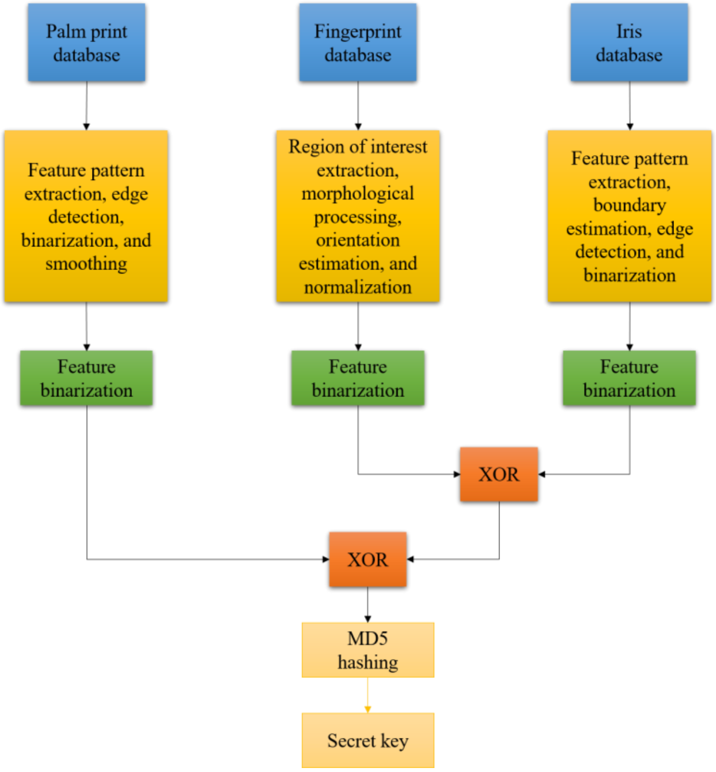
Palm print database
Fingerprint database
Iris database
Feature pattern extraction, edge detection, binarization, and smoothing
Region of interest extraction, morphological processing, orientation estimation, and normalization
Feature pattern extraction, boundary estimation, edge detection, and binarization
Feature binarization
Feature binarization
Feature binarization
XOR
XOR
MD5 hashing
Secret key

Fig. 4. The process of generating secret keys

As shown in Fig 4, the fingerprint, iris, and palm print were chosen as the biometric traits for MultiFusionGuard due to their unique characteristics and high reliability in identity verification. Fingerprint patterns are widely recognized for their distinctiveness and permanence, making them a popular choice for authentication systems. Iris patterns, being highly complex and unique to each individual, offer a robust method for user identification, even in highly secure processes. Palm prints, with their intricate patterns and variability, provide an additional layer of security in the authentication process. By leveraging these three biometric traits, MultiFusionGuard ensures a multi-layered approach to authentication, enhancing security measures within cloud computing environments. Moreover, the utilization of multiple biometric modalities adds an extra level of resilience against unauthorized access attempts, thereby fortifying data protection and mitigating various security threats inherent in cloud-based collaborative software services.

4. Simulation

The National Institute of Standards and Technology developed the Data Encryption Standard (DES) algorithm. It represents a symmetric encryption algorithm that was extensively utilized prior to the adoption of the Advanced Encryption Standard (AES). The fundamental structure underpinning DES is the Feistel cipher, forming the basis of its implementation. Within DES, a Feistel structure with 16 round patterns is adhered to, employing a block size of 64 bits. However, the optimal key length is set at 56 bits because, during the encryption process, DES disregards 8 bits from the 64-bit key. The fundamental elements of DES consist of initial/final permutation, key schedule, and round function. An important problem related to DES is its vulnerability to exhaustive key search, a technique employed in cryptoanalytic attacks to undermine the security of data encrypted using DES.

In this study, indicators of incorrect rejection ratio, incorrect acceptance ratio, and execution time are interconnected in evaluating the effectiveness of the proposed system by providing a comprehensive assessment of its performance and reliability. The incorrect rejection ratio measures the rate at which legitimate users are incorrectly denied access, while the incorrect acceptance ratio measures the rate at which unauthorized users are incorrectly granted access. These metrics reflect the system's accuracy in distinguishing between genuine and unauthorized users, which is crucial for ensuring data security. Furthermore, the execution time indicates the efficiency of the authentication process, as shorter execution times signify faster user verification. By examining these interconnected indicators, the effectiveness of the proposed system can be demonstrated: low incorrect rejection and acceptance ratios coupled with minimal execution time indicate a robust and efficient authentication system, capable of accurately verifying users while maintaining optimal performance. These specific metrics were chosen due to their direct relevance to system accuracy, security, and efficiency, providing a comprehensive evaluation of the proposed system's effectiveness in enhancing cloud security.

The AES stands as a widely acknowledged symmetric key cryptographic algorithm, renowned for its application in various security implementations. AES demonstrates a notable advantage in terms of speed, being approximately six times faster than the Triple DES algorithm. AES addresses one of the limitations of DES, which is its small key size, by using a 128-bit key for encrypting data. The utilization of a larger key size contributes to increased complexity, rendering the system more resistant to decryption attempts. Furthermore, AES supports key sizes that can be extended up to 192 and 256 bits, further enhancing its robustness against attacks. The working process of AES is iterative, incorporating Substitution and Permutation as pivotal components. AES operates its calculations in bytes, facilitating the construction of matrices. The quantity of iterations in the AES algorithm is determined by the size of the encryption key. AES uses 10 rounds for a 128-bit key, twelve rounds for a 192-bit key, and fourteen rounds for a 256-bit key. An outstanding attribute of AES is its resistance against successful attacks thus far, showcasing the strength and security of the algorithm. Currently, no notable successful attacks have compromised AES, solidifying its reputation as a highly secure encryption standard.

The Blowfish encryption algorithm, a symmetric key cryptographic system, emerged as a replacement for the DES algorithm. Its key length spans from 32 bits to 446 bits, offering versatility in key sizes. Employing a block size of 64 bits, Blowfish operates within a Feistel cipher structure, completing 16 rounds of encryption. Blowfish is widely acknowledged for its exceptional speed, making it among the swiftest block ciphers in the realm of symmetric algorithms. Nevertheless, 64-bit blocks utilized in Blowfish, less than half the size of AES's block size, make it vulnerable to particular cryptoanalytic attacks under specific circumstances. To address these vulnerabilities, a related cryptographic algorithm, Twofish, was developed as a successor to the Blowfish algorithm. The proposed methodology uses unique image processing strategies to extract features from three distinct traits. Afterwards, these characteristic points are transformed into binary equivalents to enable XOR operations between attributes. Initially, XOR operations are performed between iris and fingerprint records, generating a binary vector. This vector undergoes further XOR operations with the vector containing the binarized palm print. The resultant secret is transformed into characters and integers by MD-5 hashing, producing a confidential key for the purpose of encrypting and decrypting data. The MD-5 algorithm typically generates a binary key size of 256 bits. DES uses the initial 56 bits for data encryption, whereas both AES and Blowfish utilize the initial 128 bits. This integration of cryptographic techniques and key handling demonstrates a layered approach to ensure secure data transmission and storage.

The model was assessed using standard metrics like False Acceptance Rate (FAR) and False Rejection Rate (FRR). Figs 5 and 6 report the evaluation results, indicating that the fused features, followed by the individual iris, palm print, and fingerprint traits, exhibit superior performance in both FAR and FRR metrics. Fig 7 presents a comparison of three symmetric key encryption techniques based on their execution time, using various file sizes. DES exhibits lower execution time due to its smaller key and block sizes, while AES, despite its longer execution time, provides higher security and integrity. Blowfish maintains stable performance between DES and AES. Considering the complexity and computational steps involved, AES is identified as the algorithm that provides better security. Blowfish is considered next in line, while DES is perceived to offer the least security among the three algorithms.

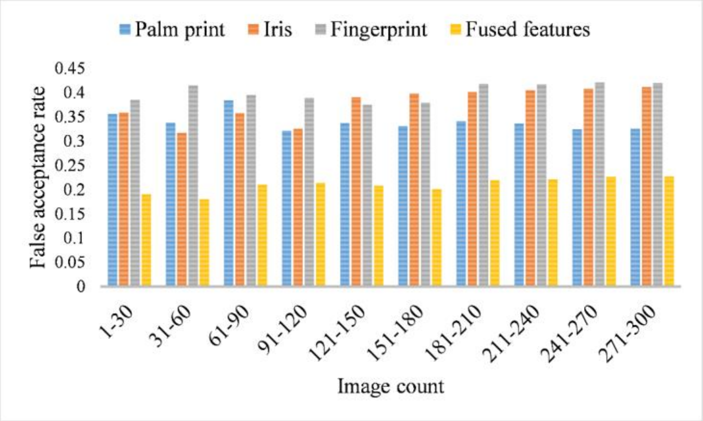

Fig. 5. False acceptance rate comparison

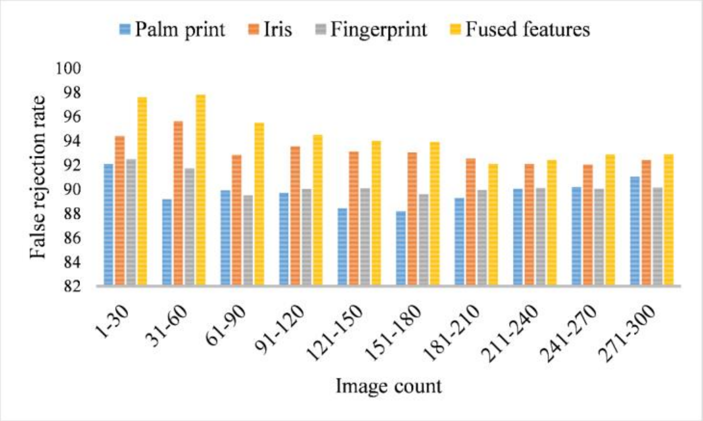

Fig. 6. False rejection rate comparison

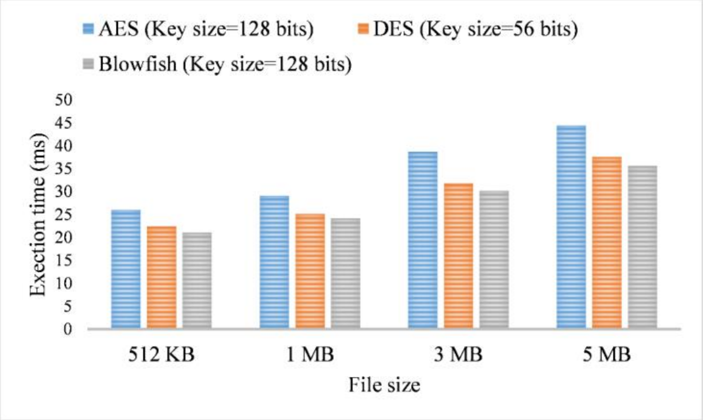

Fig. 7. Exaction time comparison

5. Conclusion

In conclusion, MultiFusionGuard stands as a groundbreaking advancement in cloud security, offering a multifaceted solution to address pressing challenges in data protection. By integrating multiple biometric modalities such as fingerprint, iris, and palm print, the framework enhances authentication mechanisms, ensuring robust user verification in cloud environments. Additionally, the incorporation of cryptographic algorithms further fortifies data security, safeguarding against unauthorized access and data breaches. MultiFusionGuard's ability to mitigate current challenges in cloud security, including concerns regarding authentication accuracy, data confidentiality, and integrity, positions it as a pivotal tool in fortifying data protection. Its potential impact extends beyond mere authentication enhancements, promising to establish a resilient defense against evolving threats and bolstering the overall security posture of cloud-based systems. As organizations continue to rely on cloud computing for critical operations, MultiFusionGuard emerges as a crucial asset in safeguarding sensitive data and mitigating risks, thereby paving the way for a more secure and resilient cloud computing landscape.

The collaborative cloud business model enables third-party software vendors to deploy their software in the cloud and offer computing services to their customers. In order to conFig cloud-based collaborative software services securely, scalable architectures with efficient authentication are required. This has led to a gradual increase in the usage of cloud services. However, it also raises concerns regarding data security. Incorporating multimodal biometric systems fortifies authentication mechanisms by leveraging unique biological patterns inherent in individuals. Such systems accurately discern individuals based on distinct patterns obtained from their traits. Furthermore, this concept finds application across various domains, enhancing system robustness. For example, it ensures the protection of human genetic codes, organizes health information for future use through Electronic Health Record (EHR) systems, and enables the management of digital ledgers. This research introduced a method of using multiple modes of biometric authentication to enhance the security of data in cloud environments. The approach relies on combining characteristics encapsulated in palm print, iris, and fingerprint attributes in order to build a confidential key. The key is then converted into a hash consisting of characters and numbers using the MD-5 hashing method. Protected data is subsequently encoded using the confidential key and three cryptographic algorithms: Blowfish, AES, and DES. DES indicates higher performance among these algorithms, whereas AES offers greater performance compared to the other two algorithms due to its powerful encryption capabilities. The incorporation of several human modalities into this security framework showcases the model's resilience in protecting the integrity of data.

REFERENCES

[1] Y. Xiaoqing, “Nature-Inspired Optimization for Virtual Machine Allocation in Cloud Computing: Current Methods and Future Directions,” *Nature*, vol. 14, no. 11, 2023.

[2] V. Hayyolalam, B. Pourghebleh, A. A. Pourhaji Kazem, and A. Ghaffari, “Exploring the state-of-the-art service composition approaches in cloud manufacturing systems to enhance upcoming techniques,” *The International Journal of Advanced Manufacturing Technology*, vol. 105, pp. 471–498, 2019.

[3] V. Hayyolalam, B. Pourghebleh, M. R. Chehrehzad, and A. A. Pourhaji Kazem, “Single-objective service composition methods in cloud manufacturing systems: Recent techniques, classification, and future trends,” *Concurr Comput*, vol. 34, no. 5, p. e6698, 2022.

[4] Z. Yang, L. Li, F. Gu, and X. Ling, “Dependable and reliable cloud-based architectures for vehicular communications: A systematic literature review,” *International Journal of Communication Systems*, vol. 36, no. 7, p. e5457, 2023.

[5] V. Hayyolalam, B. Pourghebleh, and A. A. Pourhaji Kazem, “Trust management of services (TMoS): investigating the current mechanisms,” *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 10, p. e4063, 2020.

[6] M. E. Hussain and R. Hussain, “Cloud Security as a Service Using Data Loss Prevention: Challenges and Solution,” in *International Conference on Internet of Things and Connected Technologies*, Springer, 2021, pp. 98–106.

[7] H. N. Alshareef, “Current Development, Challenges, and Future Trends in Cloud Computing: A Survey,” *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 3, 2023.

[8] A. H. A. Al-Jumaili, R. C. Muniyandi, M. K. Hasan, J. K. S. Paw, and M. J. Singh, “Big data analytics using cloud computing based frameworks for power management systems: Status, constraints, and future recommendations,” *Sensors*, vol. 23, no. 6, p. 2952, 2023.

[9] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, “Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm,” *Mater Today Proc*, vol. 37, pp. 2653–2659, 2021.

[10] M. Mayuranathan, M. Murugan, and V. Dhanakoti, “Enhanced security in cloud applications using emerging blockchain security algorithm,” *J Ambient Intell Humaniz Comput*, vol. 12, pp. 6933–6945, 2021.

[11] 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 (N Y)*, vol. 433, pp. 431–447, 2018.

[12] N. D. Sarier, “Multimodal biometric authentication for mobile edge computing,” *Inf Sci (N Y)*, vol. 573, pp. 82–99, 2021.

[13] A. Gumaei, R. Sammouda, A. M. S. Al-Salman, and A. Alsanad, “Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation,” *J Parallel Distrib Comput*, vol. 124, pp. 27–40, 2019.

[14] B. M. Singh and J. Natarajan, “A novel secure authentication protocol for ehealth records in cloud with a new key generation method and minimized key exchange,” *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 7, p. 101629, 2023.

[15] A. K. Singh, A. Nayyar, and A. Garg, “A secure elliptic curve based anonymous authentication and

key establishment mechanism for IoT and cloud," *Multimed Tools Appl*, vol. 82, no. 15, pp. 22525–22576, 2023.

[16] S. Shukla and S. J. Patel, "A novel ECC-based provably secure and privacy-preserving multi-factor authentication protocol for cloud computing," *Computing*, vol. 104, no. 5, pp. 1173–1202, 2022.

[17] N. Santos, B. Ghita, and G. Masala, "Medical Systems Data Security and Biometric Authentication in Public Cloud Servers," *IEEE Trans Emerg Top Comput*, 2023.