Algorithm Policy for the Authentication of Indirect Fingerprints Used in Cloud Computing

Anusha Bodepudi[1]*, Manjunath Reddy[2], Sai Srujan Gutlapalli[3], Mounika Mandapuram[4]

[1]Staff Engineer, Intuit, Plano, TX, **USA**
[2]Customer Engineering Lead, Qualcomm, San Diego, CA, **USA**
[3]Data Engineer, TechnoVision Solutions LLC, Farmington Hills, MI 48335, **USA**
[4]EKIN Solutions, 13800 Coppermine Rd, Herndon, VA 20171, **USA**

E-mail for correspondence: anusha_bodepudi@intuit.com

ABSTRACT

User identity identification secures cloud computing. This study examined cloud service security authentication needs. Fingerprint recognition was used to create a new cloud security authentication system. The proposed system's design and process were thoroughly examined to secure cloud user data from unauthorized access. This study proposes a secure cloud server fingerprint match technique. Considering fingerprint uniqueness and stability, cloud security login authentication technology employing fingerprint recognition is researched to improve cloud services login security. Analyze the cloud security login system structure first. Next, fingerprint identification is explained. Finally, fingerprint identification of cloud security login systems is investigated from fingerprint registration, certification, fingerprint image processing perspectives, and a simple fingerprint image processing simulation. The results show that this login mechanism is secure and versatile. The biometric template is insecure, and stolen templates cannot be canceled, making user identity leaks easy. This work proposes indirect fingerprint authentication to address these issues. Finally, a thorough security analysis of the cloud computing method is offered.

Keywords: Computer Information Security, Certification, Cloud Computing, Fingerprints, Authentication, Character Recognition

INTRODUCTION

The authentication of the actual user is of the utmost importance in situations when the apps include handling money, such as the Internet or mobile banking. Authentication of users is a critical component in some different applications (Yassin, 2014). In the past, secret values such as passwords and PIN numbers were utilized for the purpose of recognizing verified users. However, it is tough to recall all of them. Users benefit greatly from the convenience of biometric systems because it is unnecessary to remember any explicit information (Thodupunori & Gutlapalli, 2018). However, in contrast to passwords, the values of a person's biometrics cannot be altered if there is a concern that they may have been compromised. Cancellable biometric systems are being offered to provide adequate protection for biometric fields. In these schemes, the biometric information is first subjected to an algorithm, which is then saved. During the verification process, the distorted data are corrected before being compared to the user's biometric information (Pang et al., 2013). Generating a one-of-a-kind number from the biometric feed and storing only that number in place of the accurate biometric data is an additional method that can be utilized to conduct biometric authentication without running the risk of losing the data. Cloud storage provides a vast amount of capacity for the data storage needs of enterprises. Using a feature extraction method known as the SURF (Speeded Up Robust Features) scheme, we will show our method that produces a unique number for a fingerprint template. This method will be discussed in this paper. The FINs that are created are uploaded to a cloud storage service. Every time a user wishes to log into his eHealth system, he must submit his fingerprint, which is immediately turned into a FIN, sent to the cloud server, and compared to the previously saved FIN. Our implementation on MatLab yielded satisfactory results, meaning that we could effectively authenticate users using the critical value obtained by our technique (Wu et al., 2014).

The Internet of Things (IoT) is undergoing tremendous expansion, and behind this comes the concomitant difficulty of protecting users' personal information and data privacy (Reddy et al., 2020). The usual cryptography and personal authentication systems for cloud-assisted IoT could be strengthened with the help of biometric recognition technologies, which are both interesting and promising. In the event that the biometric information is stolen or otherwise compromised, there is no simple way to cancel or replace it. This research suggests a fingerprint identification system that uses a minutiae-based sector coding strategy for use with the cloud-assisted Internet of Things (Gutlapalli et al., 2019). The scheme is based on fuzzy commitment protocol. In our method, the minute details of a fingerprint are broken down into many different sectors that have been designed, and they are then encoded according to the characteristics of those sectors. The procedure of key encryption is carried out by utilizing BCH codes and Hash mappings. This is made possible by the concept of fuzzy commitment. Not only does our strategy offer a flexible way to realize fingerprint recognition between complexity and security by designing error-correcting codes with different parameters, but it also offers a good balance between the genuine accept rate (GAR) and the false acceptance rate (FAR) with customized sector coding strategies (Mandapuram, 2017). Our scheme's ability to design error-correcting codes with different parameters makes this possible.

The rapid rise in the number of security problems involving cloud computing highlights both this technology's benefits and difficulties. The integration of mobile technology with cloud computing and mobile biometric authentication in cloud computing is given in this study as a potential solution to this challenge (Mandapuram & Hosen, 2018). Since mobile cloud computing is becoming increasingly popular among mobile users, biometric authentication is being implemented as an additional layer of protection. This study aims to investigate the application of mobile cloud computing (MCC) in the context of a security problem using a finger biometric authentication paradigm. The entropy value generates the secret code through this fingerprint biometric. This allows the person to request access to the data stored on the desk computer (Mandapuram et al., 2018). When a person requests access to an authorized user via Bluetooth in their mobile device, the authorized user will submit the permit access using a fingerprint secret code. The final step is to compare this fingerprint with the database that is stored on the desk computer. If the two are compatible, the requested user will be granted access to the computer.

Statement of the Problem

Cloud computing is internet-based computing that gives users and other devices access to shared resources, software, and data as needed. Despite the potential benefits of cloud computing, its security still needs to be improved, hindering the cloud model's adoption. As a result, the need for a reliable user authentication method has grown as networking, communication, and mobile technologies evolve quickly, and security issues have grown more serious.

The biometrics essential release, creation, and binding are three crucial phases in biometrics cryptosystems. First, only the authorized user can obtain the key if the biometric matching is successful in primary release mode. In the critical generation mode, we obtain the cryptographic system's key from the biometric template. This creates a foundation for safe systems due to the distinctive biometric findings based on some feature or transform extraction. If not, the database does not store the key. Instead, a cryptosystem framework monolithically binds the key and the template in the critical binding mode. Decoding the key or the template with access to the user's biometric information is possible. Because user authentication and critical release are two different processes in the vital release mode, which increases the unsafe elements in the authentication scheme, the primary generation/binding mode is more secure than the key release option. Finally, we describe a fuzzy vault implementation based on the fingerprint-based fuzzy vault to secure the particular minutiae feature values as the private key derived from the fingerprint template. This study combines the fingerprint template features with the suggested safe authentication system. We then apply the critical binding mode to that combination.

The critical implementation problem is the alignment of the query fingerprint to the original template because the fuzzy vault approach suggested by Juels and Sudan only saves an altered version of the fingerprint template. The scheme's implementation keeps high curvature points from the template fingerprint's orientation field as helpful information to aid alignment. While precisely aligning the template and query details, the helper data does not divulge any private information about the template.

Fingerprint Index Management Model

As the amount of data stored in data centers continues to increase, cloud storage models are encountering increasing challenges while storing data and providing the capabilities required to move data in an appropriate amount of time (Gutlapalli, 2017). This research aims to create a model for distributed data duplication that can achieve scalable throughput and capacity by leveraging a large number of data servers to duplicate data in parallel with a small amount of data being lost. A new approach for cloud storage that is based on distributed data duplication and fingerprint index management (DDFI) is proposed in this research. The DDFI paradigm consists of three primary stages of operation. When the DDFI model is first implemented, it uses an efficient routing strategy determined by the similarity level of the data. This results in low network overhead due to the early identification of storage locations. In the second stage, the MD5 algorithm is used to carry out the method for identifying duplicate data. This procedure is carried out in the second stage. In the final step, a fingerprint index management procedure is carried out. This process involves the creation of a fingerprint index, which includes fingerprints and the position details relating to each written chunk. The DDFI model is responsible for managing the fingerprint index in storage space, and it only occasionally writes to disk at the same time that the cloud database scheme is idle. This helps to ensure that the results of the deduplication performance are optimized. The simulation results demonstrated that the presented DDFI model provided maximum results with a more excellent deduplication ratio (DR) while requiring a minimal increase in network bandwidth. It can be deduced from the comprehensive comparison study that the presented DFFI model provided the highest possible relative DR, the highest possible duplication performance, the lowest possible read bandwidth, and the highest possible write bandwidth.

Why Is the Cloud Authentication Important

The cloud is used for most of the world's information technology and data-driven businesses. However, it should be clear that this is the case when one considers that infrastructure offers a degree of adaptability, resiliency, and scalability that most enterprises will not find in conventional on-premises solutions (Dassouki et al., 2017).

The cloud presents many of the same concerns in terms of security and compliance as on-premises technology did. In many cases, the difficulty of these problems is even more significant in the cloud (Juels and Sudan, 2002). This is because the infrastructure, which includes apps, analytics, and tools, must have a connection to users that is secure and compliant without compromising the usefulness of the link. In addition to this, these ecosystems are both diverse and widespread around the world (Pang et al., 2013). Users in every location can derive genuine benefits from the collaborative efforts of numerous security-related components and solutions. This is a severe problem.

Using authentication in the cloud becomes relevant at this point (Yang et al., 2011). Cloud verification, which is quite similar to traditional authentication, is a system that verifies users' identities before granting access to services. Users validate their identities by providing credentials before gaining access to apps and other services provided by the operating system.

Nevertheless, there are a few obstacles that cloud-based identification must overcome:

- Password Security: Database lookups are a frequent approach to confirm passwords. Hackers can quickly grab passwords from these lookups. Most users reuse passwords across platforms and accounts, compounding this issue. Regardless of credentials management, many accounts on various services increase a user's data attack surface.
- Distributed environments are a set of hardware, tools, and configurations. LDAP, Kerberos, database lookups, and others can likely validate credentials. This makes it harder to manage users across systems safely.
- Transparency and Privacy: Corporate users need help to grasp their risk profile on many platforms. If possible, a supplier could obstruct such comprehension by making procedures difficult for users to grasp. Moreover, cloud computing's distributed nature makes it difficult to authenticate a user's identity.

Switching to a different method of identity verification is one of the most significant breakthroughs in authentication that helps providers handle these issues.

The Fingerprint-based Fuzzy Vault (FFV)

The fuzzy vault architecture is a biometric cryptosystem that protects the secure key and the biometric template by binding them within a cryptographic framework (Dassouki et al., 2017). This keeps both of these sensitive pieces of information safe. The fingerprint minutiae form the foundation of the fully automatic execution of the fuzzy vault technique discussed earlier. The fuzzy vault merely maintains an altered version of the template. To align the query fingerprint, it employs the retrieved high curvature points generated from the fingerprint orientation field as the assistance data.

Given that the helper data are kept as public information, it is not appropriate for it to disclose any confidential information regarding the template. On the other hand, ought to include enough information to ensure precise alignment. The unique minutiae feature values that serve as the private key are derived from the user's fingerprint by the system when the user registers by putting his finger on the sensor (A Amali & Rama, 2017). The fingerprint template and the private key will be used as the encoding data during the vault encoding process. This will cause the vault value and the helper data (HD) to be generated (Kalangi & Rao, 2018). The user must then save the encoded data to the USBKEY. When the user needs to retrieve the private key, they will touch the sensor with their finger again (Jiang & Zheng, 2014). The system produces the query helper data, also known as QHD, and then both QHD and HD are utilized to align the template and the query fingerprint properly. After then, the process of decoding the vault will use the vault value that is stored in USBKEY to determine whether or not the input fingerprint is legitimate. The private key will be output if there is no error during detachment (Bodepudi et al., 2019). There is no matching in this area, and several of the processes look like they will take a long time. As a result, we shall use this foolproof strategy throughout this paper.

Security and Functionality Analysis

In Cloud Computing, misuse of access authority to resources and leak of personal information used to authenticate users could affect faster and more potent than a mono-system (Rajarajan et al., 2019). This study proposes a Cloud Computing security authentication system. This section will show how the suggested authentication mechanism resists two typical assaults. Gupta, M. Quamara, and other architectures are compared to the proposed one. The comparison analysis suggests a few outcomes of the proposed architecture:

- The malfunction of a reliable server hosted by a third party was the cause of the delay that occurred in the earlier works. The registration process for employing biometrics is relatively straightforward compared to other authentication methods, and a trusted third party will not be involved in the authentication process. Consequently, the suggested design has the potential to lower this cost.
- The vulnerability of cloud computing to attacks on its security and privacy is significantly reduced thanks to biometric authentication and the utilization of public key cryptography.
- Architecture is suited for resource-constrained end devices used in cloud computing environments because there is no high processing of information, exponential calculation process during authentication, and no additional workloads, such as changing a password. This is because there is no high processing of information.
- A single user agent can only have one account for all the cloud application services they utilize, eliminating the need for phony user accounts or redundant accounts in the cloud. There is a direct correlation between the individual user and the cloud service.
- Using a biometric approach, there will be no loss of information stored in the cloud (even if the user's smart card is lost); users can modify their fingerprint choice in the Remote Verification System (RVS) using a secure password.
- An adversary attempting to replicate the fingerprint by utilizing a mark-tracked print will be unable to access the services that need mutual authentication. This is because OTP is only provided to the devices of users who have registered for such services.
- < UNK> Using the status bit prevents hostile users from logging in many times with the same user credentials, significantly reducing the risk of a DOS attack.
- The user can modify their chosen finger number at any time by simply sending a request to RVS while logging in with their password.
- RVS does not involve itself in the authentication of the user every time; as a result, the complexity of the computing process is reduced.

Proposed Scheme for Indirect Fingerprint Authentication

This section demonstrates a practical implementation of the indirect fingerprint authentication scheme (IFAS) based on FFV and PKI. The proposed method utilizes the user's fingerprint as the indirect authentication credentials and the key binding mode scheme FFV to accomplish the binding generation mode effect. This effect allows the user's fingerprint to produce a secret key unique to that user and serves as the user's private key.

Specifications

The following is a list of the proposed scheme's criteria and parameters:

- Presumably, unauthorized parties cannot easily steal and replicate fingerprint pictures.
- The template of the user's fingerprints is used as the seed for the private key.
- The USBKEY includes a working area and a storage region, neither providing any security risks. As a result, any generated data can quickly and easily be purged from the system during authentication.
- The IFAS mechanism that has been proposed can be inserted into the USBKEY.
- PKG stands for "private key generator center" and refers to a facility housed within Bio-CA. It is presumed that this organization is a legitimate one.
- This study uses a biometric certification authority (Bio-CA) based on the existing PKI.

Registration Phase

Everyone who uses the system legally must go through the process of registering their fingerprints at the PKG facility. During registration, a private key is initially generated from the user's fingerprint, and then the public key that corresponds to the private key is derived from the private key (Alsmirat et al., 2019). The user must provide the Bio-CA with the user's information and the public key to register for an account. The user is presented with a public key certificate from the Bio-CA if and only if the Bio-CA can successfully validate the user's identity. After that, in order to initialize the USBKEY, the PKG will use the user's private key and fingerprint template to produce the vault value and help data, respectively. After all of the information, including the public key certificate, has been saved in the storage area of the USBKEY, it is then given to the person authorized to access it.

Authentication Phase

When a user wants to sign a message (generated by USBKEY as a random number), the user inputs his or her fingerprint using the USBKEY sensor. The vault's decoding procedure will produce the user's private key if the user is verified as legitimate. The message has been digitally signed using the secret key.

An Implementation of Cloud Computing

Transport Layer Security, also known by its more general term "Secure Sockets Layer (SSL)," has been implemented. It comprises two primary components: The TLS Handshake is used to authenticate both the server and, if necessary, the client. The Record Layer is responsible for encrypting and decrypting TCP data streams using the methods and keys that were negotiated during the TLS Handshake. Because it is incorporated into every online browser, it is currently the most critical cryptographic protocol globally. In addition, TLS gives users various alternatives regarding crucial negotiation, encryption, and authentication of cloud computing network partners. As a consequence of this, we can configure the web browser with trustworthy certificates in order to communicate with the server that manages the cloud environment.

FINGERPRINT VERIFICATION

Biometrics-based individual authentication schemes that use physiological biometrics like eye recognition, fingerprint, or behavioral actions like speech and handwriting traits are becoming more popular than conventional systems that use e-tokens (e.g., RSA-token) or knowledge like passwords. Conventional authentication systems cannot distinguish between honest users and attackers who illegally get access privileges. Biometric authentication techniques are also better for consumers because there is no password to forget or token to lose, and a single biometric property, like a fingerprint, can be used to access several accounts without a password. Age-related fingerprints are difficult to distinguish. Thus, fingerprint biometric authentication is the most researched and developed. Fingerprint identification is a popular biometric. Ridge lines flow parallel, creating a pattern. According to Galton, each ridge is categorized by minute individualities called minutiae, which may split and almost directly reunite, enclosing a small spherical or elliptical space or sometimes the autonomous beginning or termination of ridges. Ridges are black, valleys light. Ridges and valleys sometimes run parallel, bifurcate, or terminate. Finally, depending on sensor resolution and finger placement, a good fingerprint must have 25–80 minutes. Briefly, fingerprint technology considers a complex pattern recognition issue. Designing algorithms that can firmly extract and match significant features is difficult, especially in low-quality fingerprint photos. Since it was initially used in pattern recognition about fifty years ago, self-propelled fingerprint identification is often thought to have been solved. The fingerprint method remains a complex and crucial pattern recognition challenge.

Thus, fingerprint verification involves enrollment and verification. The user enrolls his fingerprint as a template to the server, which extracts features. The server compares a user's fingerprint data to the template to verify their identity. Traditional fingerprint systems require additional hardware and software for user logging. This work proposes a new user verification system without software for input fingerprint, preprocessing images, feature extraction, classification, and verification. Unfortunately, our technique does not require fingerprint-reading hardware for each user's logging system. Most biometric fingerprint authentication solutions use minutiae (level 2 features). Ridge termination and bifurcation are the most notable minutiae. High-accuracy fingerprint scans and enough fingerprint surface area make minutiae-based systems work well (Gupta & Quamara, 2018). These prerequisites may never be met. Often, only a tiny portion of the test fingerprint matches the reference fingerprint. Due to low interference between fingerprint gains from small-area sensors, comparing fingerprints is difficult. Fingerprints are distinct patterns of ridge and valley points on a finger. Valleys are between two ridges, and ridges are single curving sections. Bifurcations and ridge ends are local ridge cavities represented by minutiae points. Good fingerprint images have 40–100 minutiae. These tiny dots continuously identify a user's fingerprint. The first part processes a raw fingerprint image and extracts fingerprint features, the details.

DISCUSSION ON FINDINGS

Cloud computing service providers are spreading worldwide to give users appropriate resource processing and storage (Zhang, 2013). This study explores cloud computing security utilizing fingerprint-based biometric authentication. The architecture reduces cloud computing security attacks and removes phony accounts by requiring fingerprint-based identification upon registration. The suggested algorithm leverages several cloud application services and enables single SSO login for resource-constrained end devices to access cloud services. Fingerprint-based authentication is vulnerable because users can leave their fingerprints on any surface, which attackers can use for authentication (Shi et al., 2019). Finger pulse rate solves vulnerability. Implementing the framework and doing an AVISPA performance analysis may validate the recommended architecture. SIP is a prominent VoIP signaling protocol. Live deployment proved its flooding weakness, like other Internet protocols. These application-level attacks are analogous to TCP protocol exploits. This study introduces a new SIP device flooding defense. Our proposed approach uses two algorithms:

- A detection algorithm that considers the SIP protocol's temporal characteristics and the fingerprints of its messages, and
- A mitigation algorithm that filters SIP communications based on a fingerprint allowlist database. Both of these algorithms are necessary to protect against an attack fully.

We compare our technique to previous approaches in the literature using broadly distributed cloud virtual machines. The trials simulate a massive flooding attack from faraway data centers. The results show fast detection, few false alarms, and efficient computational resource reduction.

Today, cloud computing allows individuals and companies to store, process, and distribute data cheaply on external servers (Tang et al., 2015). Cryptography, biometrics, PKI, and cloud standards can assist us in overcoming security issues. Biometric systems are widely utilized for user authentication and will become part of the core information infrastructure. A wholly automatic and practical fuzzy vault achieves secure biometric authentication and critical cryptographic security (Zhang, 2013). This study introduces a fuzzy vault-based PKI indirect fingerprint remote authentication strategy for cloud computing. The suggested remote authentication biometric template security system is resilient to two prevalent threats. Thus, the indirect fingerprint authentication system is effective and secure and might be used to standardize Cloud Computing security standards for data security, administration, and protocols.

Conclusion

In today's world, authenticating and gaining access to a mobile phone with one's fingerprint has become commonplace. Because fingerprints can be easily stolen, it is not straightforward to use fingerprints as a form of authentication for remote servers. In this article, we provide a cloud-based fingerprint authentication system capable of converting a user's fingerprint into a one-of-a-kind FIN and carrying out the verification in the cloud. However, recreating the fingerprint using the FIN as a guide is impossible. We analyzed to see whether or not the proposed plan was sound, and we came to that conclusion. The variances in the fingerprints are something that we aim to investigate in further studies. Experimenting with the presented method on iris data is another possible direction for future investigation. Because the value of an iris does not change, unlike fingerprints, it is possible that it would make a superior contender.

Cloud computing has much potential for information technology organizations and gives more flexibility. Information security is one of the most critical challenges. This research proposed a customizable security method that a cloud storage owner can utilize to protect the data they store in the cloud. Fingerprint biometric authentication is offered using mobile cloud computing, and the Maximum Entropy Expectation-Maximization Algorithm is used to generate the secret code. This paper provides an identifier for cloud storage that can access data or files from a personal computer or mobile device anywhere using fingerprint recognition.

References

A Amali, M. B., & Rama, N. (2017). Biometric Identification and Authentication Providence using Fingerprint for Cloud Data Access, *International Journal of Electrical and Computer Engineering*, *7*(1), 408-416.

Alsmirat, M. A., Al-Alem, F., Al-Ayyoub, M., Jararweh, Y., & Gupta, B. (2019). Impact of digital fingerprint image quality on the fingerprint recognition accuracy. *Multimedia Tools and Applications*, *78*(3), 3649-3688. https://doi.org/10.1007/s11042-017-5537-5

Bodepudi, A., Reddy, M., Gutlapalli, S. S., & Mandapuram, M. (2019). Voice Recognition Systems in the Cloud Networks: Has It Reached Its Full Potential? *Asian Journal of Applied Science and Engineering*, *8*(1), 51–60. https://doi.org/10.18034/ajase.v8i1.12

Dassouki, K., Safa, H., Nassar, M., & Hijazi, A. (2017). Protecting from Cloud-based SIP flooding attacks by leveraging temporal and structural fingerprints. *Computers & Security*, *70*, 618.

Gupta & Quamara, M. (2018). An identity-based access control and mutual authentication framework for distributed cloud computing in the Internet of Things environment. *ICCIDS Procedia Computer Science*, 189-197.

Gutlapalli, S. S. (2017). The Role of Deep Learning in the Fourth Industrial Revolution: A Digital Transformation Approach. *Asian Accounting and Auditing Advancement*, *8*(1), 52–56. Retrieved from https://4ajournal.com/article/view/77

Gutlapalli, S. S., Mandapuram, M., Reddy, M., & Bodepudi, A. (2019). Evaluation of Hospital Information Systems (HIS) in terms of their Suitability for Tasks. *Malaysian Journal of Medical and Biological Research*, *6*(2), 143–150. https://doi.org/10.18034/mjmbr.v6i2.661

Jiang, X. C., & Zheng, J. D. (2014). An Indirect Fingerprint Authentication Scheme in Cloud Computing. *Applied Mechanics and Materials*, *484-485*, 986-990. https://doi.org/10.4028/www.scientific.net/AMM.484-485.986

Juels, A. and Sudan, M. (2002). A fuzzy vault scheme. In Proc. IEEE Int. Symp. Inform. Theroy, Lausanne, Switzerland, p. 408.

Kalangi, R. R., & Rao, M. V. P. C. (2018). A novel multi-user fingerprint minutiae-based encryption and integrity verification for cloud data. *International Journal of Advanced Computer Research*, *8*(37), 161-170. https://doi.org/10.19101/IJACR2018.837010

Mandapuram, M. (2017). Application of Artificial Intelligence in Contemporary Business: An Analysis for Content Management System Optimization. *Asian Business Review*, *7*(3), 117–122. https://doi.org/10.18034/abr.v7i3.650

Mandapuram, M., & Hosen, M. F. (2018). The Object-Oriented Database Management System versus the Relational Database Management System: A Comparison. *Global Disclosure of Economics and*

Business, 7(2), 89–96. https://doi.org/10.18034/gdeb.v7i2.657

Mandapuram, M., Gutlapalli, S. S., Bodepudi, A., & Reddy, M. (2018). Investigating the Prospects of Generative Artificial Intelligence. *Asian Journal of Humanity, Art and Literature*, *5*(2), 167–174. https://doi.org/10.18034/ajhal.v5i2.659

Pang, X., Song, Z., & Xie, W. (2013). Extracting Valley-Ridge Lines from Point-Cloud-Based 3D Fingerprint Models. *IEEE Computer Graphics and Applications*, *33*(4), 73-81. https://doi.org/10.1109/MCG.2012.128

Pang, X., Song, Z., & Xie, W. (2013). Extracting valley-ridge lines from point-cloud-based 3D fingerprint models. *IEEE Computer Graphics and Applications*, *33*(4), 73-81. https://doi.org/10.1109/MCG.2012.128

Rajarajan, S., Kausik, R., Charan, M., & PLK. Priyadarsini. (2019). Privacy-Preserving Fingerprint Authentication at the Cloud Server for eHealth Services. *EAI Endorsed Transactions on Pervasive Health and Technology*, *5*(18). https://doi.org/10.4108/eai.13-7-2018.162688

Reddy, M., Bodepudi, A., Mandapuram, M., & Gutlapalli, S. S. (2020). Face Detection and Recognition Techniques through the Cloud Network: An Exploratory Study. *ABC Journal of Advanced Research*, *9*(2), 103–114. https://doi.org/10.18034/abcjar.v9i2.660

Sabeetha, S. S., & Malarvizhi, N. (2021). Distributed deduplication with fingerprint index management model for big data storage in the cloud. *Evolutionary Intelligence*, *14*(2), 683-690. https://doi.org/10.1007/s12065-020-00395-8

Shi, S., Cui, J., Xin-Li, Z., Liu, Y., Jing-Liang, G., & Yun-Jiang, W. (2019). Fingerprint Recognition Strategies Based on a Fuzzy Commitment for Cloud-Assisted IoT: A Minutiae-Based Sector Coding Approach. *IEEE Access*, *7*, 44803-44812. https://doi.org/10.1109/ACCESS.2019.2906265

Tang, Y., Zhang, Y., & Zhang, N. (2015). Cloud Security Certification Technology Based on Fingerprint Recognition, *Telecommunications Science*, *31*(8).

Thodupunori, S. R., & Gutlapalli, S. S. (2018). Overview of LeOra Software: A Statistical Tool for Decision Makers. *技术与管理回顾*, *1*(1), 7–11. http://技术与管理回顾.移动/index.php/tmr/article/view/4

Wu, H., Fan, J., Liu, J., & Zhang, J. (2014). Cloud Storage Data Protection Mechanism Based on a Fingerprint Cube Algorithm. *Telecommunications Science*, *30*(11), 110-115. https://doi.org/10.3969/j.issn.1000-0801.2014.11.019

Yang, J., Xiong, N., Vasilakos, A. V., Fang, Z., Park, D., Xu, X., Yoon, S., Xie, S., & Yang, Y. (2011). A Fingerprint Recognition Scheme Based on Assembling Invariant Moments for Cloud Computing Communications. *IEEE Systems Journal*, *5*(4), 574-583. https://doi.org/10.1109/JSYST.2011.2165600

Yassin, A. A. (2014). Efficiency and Flexibility of Fingerprint Scheme Using Partial Encryption and Discrete Wavelet Transform to Verify User in Cloud Computing. *International Scholarly Research Notices, 2014.* https://doi.org/10.1155/2014/351696

Zhang, X. (2013). Design of Cloud Security Login System Based on Fingerprint Recognition, *Dianshi Jishu (Video Engineering)*, *37*(13), 166-171.

Zhang, X. (2013). Design of Cloud Security Login System Based on Fingerprint Recognition. *Dianshi Jishu (Video Engineering)*, *37*(13), 166-171.

--0--

Archive Link: **https://abc.us.org/ojs/index.php/ajtp/issue/archive**