

Crypt analysis of multi-key biometric encryption for business enterprises using cloud storage

Sahil Rampal [@]

Manmohan Sharma [†]

Parul Khurana [§]

Department of Computer Applications

Lovely Professional University

Punjab 302032

India

Mukesh Kumar [#]

Department of Computer Applications

Chandigarh School of Business

Chandigarh Group of Colleges

Jhanjeri

Mohali 140307

Punjab

India

Vivek Bhardwaj ^{*}

Department of Computer Science and Engineering

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Abstract

In the current competitive global scenario, cloud computing is an important tool for running successful businesses. Cloud computing has become the model for data storage and running applications from distant locations using pay-per-use infrastructure. Cloud users are not in direct control of their data, thus making the operations used to manage

[@] E-mail: sahil.rampal@gmail.com

[†] E-mail: manmohan.sharma71@gmail.com

[§] E-mail: parul11183@gmail.com

[#] E-mail: mukesh.kumarphd2014@gmail.com

^{*} E-mail: vivek.bhardwaj@jaipur.manipal.edu (Corresponding Author)

data security more challenging. Data encryption at the data source can prevent data leakage while in transit and data tampering when stored in the cloud. Business data encryption using single biometric encryption techniques sometimes fails, as single biometric features can become distorted or compromised. Conversely, the use of multiple biometrics for encryption can provide a better solution. This paper suggests multi-key multi-modalities biometric encryption techniques for businesses to secure important data stored on local premises or offloaded to the cloud. To enhance security, data is encrypted with a master key derived from multiple user keys. To decrypt the data, at least a threshold (t) number of keys are required to generate the master key to decrypt the data.

Subject Classification: Primary 68P25, Secondary 94A60.

Keywords: Multi-modalities biometric encryption, Cloud data security, Business application data, Multi-key encryption, Biometric-fusion, Key-hashing.

1. Introduction

Cloud computing, a rapidly evolving field within computer science, has transformed the landscape of data storage and application management. Its adoption has been fuelled by the myriads of benefits it offers, including cost-effectiveness, scalability, and accessibility. Businesses across various sectors have leveraged cloud computing to streamline their operations and improve efficiency. Cloud computing has changed the way business acquire and use infrastructure and services to perform their day-to-day operations [1] [2]. It became the model for data storage and running application from a distant place using infrastructure as pay per use model. In cloud computing the hardware infrastructure is owned and managed by a cloud service provider, who is responsible for up keeping of the infrastructure being used as cloud services. Therefore, cloud service user needs not to develop their own infrastructure for starting any initiative, which in terms reduce the cost of the initiative. furthermore, cloud user leverages the benefits of extending their hardware requirements without making provisioning plans to add up additional hardware to keep up the initiative [3] [4]. These benefits led to more successful business start-ups. However, as the utilization of cloud services continues to grow, so do the challenges associated with it. One of the most pressing issues is security. The increasing number of cyber-attacks targeting cloud infrastructures has raised serious concerns about the safety and integrity of data stored in the cloud. A security breach in any cloud service can result in significant costs for both the cloud provider and users. Currently, no cloud system—whether public, private, community, or hybrid—offers robust security, leading to hesitancy among users to store sensitive data on the cloud. The

biggest challenge in cloud computing is data security from hackers and the malicious cloud service providers. Although many attempts are made to secure the cloud data, hackers are still able to breach the cloud security. Data encryption-based solutions implemented at cloud also failed to save the data while data in transit or when cloud service provider is malicious. therefore, we purpose multi-key, multi-modality biometric encryption scheme to secure the data at local premises or offloading to the cloud. In the proposed system, data is encrypted using a master encryption key obtained by integrating all the user keys, which are formed by fusing the users' multiple biometric feature vectors generated from various modalities.

2. Related Work

Thabit in [1] emphasizes the critical role of cryptographic algorithms in enhancing IoT security, particularly focusing on lightweight and hybrid ciphers to address the challenges of data protection in resource-constrained IoT environments.

Gundu [2] introduced a Multi-Key Biometric Authentication System for virtual work environments, utilizing group, pairwise, and individual keys to improve security. The study demonstrated the scheme's effectiveness against various attack models, highlighting its superiority over single-key approaches for securing remote work environments. Buyya, Yeo, and Venugopal [5] stressed the importance of developing market-oriented clouds by utilizing technologies like virtual machines. Wang et al., [6] suggested that "the control of data and application in cloud are not the same as in the case of traditional system, and the data and services managed by cloud provider cannot be trusted fully". According to Chen, Paxson, and Katz [7] many cloud computing security challenges are not entirely new or insurmountable. They highlight examples such as the complexities involved in multi-party trust and the importance of ensuring mutual auditability. Later Wang et al., [8] proposed "flexible distributed storage integrity auditing mechanism for auditing of the cloud storage for the security of cloud data" which is required to improve the confidence of the cloud users. Jagadeesan et al. [9] proposed a method leveraging multimodal biometrics, including iris and fingerprint data, to create a secure cryptographic key, enhancing security through the complexity of factoring large numbers. Kuyoro, Ibikunle, and Awodele [10] observed that despite cloud computing's transformation from a promising business idea to a rapidly expanding segment of the IT industry,

security concerns have considerably hindered its widespread adoption by customers. In the meantime, Loganayagi and Sujata [11] suggested how “combining virtualization and policy monitoring to enhance the level of cloud security”. Zissis and Lekkas [12] proposed that cloud computing merges elements from grid computing, utility computing, and autonomic computing into a new deployment model, while also inheriting the security issues related to these existing technologies. Additionally, Moritz Borgmann et al. [13] pointed out that encryption schemes can sometimes be inadequate, as some storage providers use encryption keys that they generate and store themselves. Chen and Zhao [14] emphasized that concerns over data security and privacy are significant obstacles preventing large businesses from adopting cloud computing, especially for applications that are critical to their operations. Meanwhile, Sood [15] proposed a framework that combines multiple mechanisms and available techniques to protect critical information from unauthorized access. Yong Yu et al. [16] investigated active adversary attacks within three cloud data auditing mechanisms and showed that these systems become vulnerable when such adversaries engage in cloud storage.

3. Proposed Methodology

In this competitive world, businesses require strict security practices to be followed for the data security. Businesses using cloud to store their

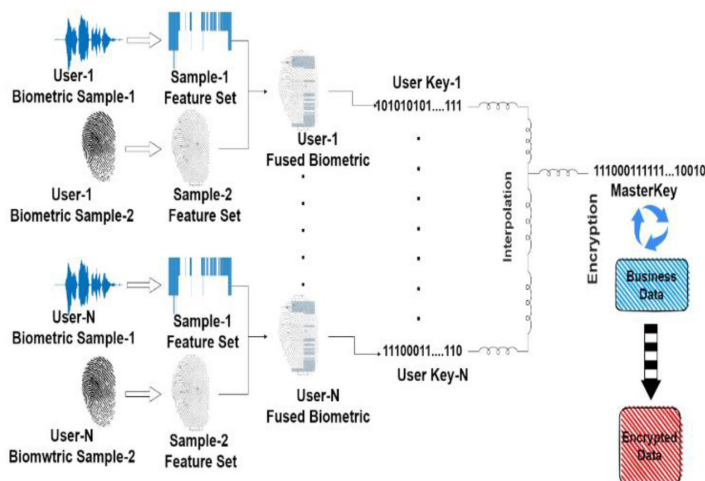


Figure 1

Multi-Key multi-modalities biometric encryption

data are heavily targeted by the hackers. Thus, there is a need to design a system where we can easily set the responsibility for the operation performed and to secure the data. Hence, we purpose multi-key multi-modality biometric encryption scheme, where selected biometric traits of multiple users are used to generate the master encryption key.

Multi-modalities biometric encryption keys (user keys) are generated for data users, and user keys are interpolated to generate the master key by Shamir's secret sharing approach by deciding the minimum number of keys (threshold) required to regenerate the master key. Polynomial of degree $t-1$ where $f(x) = a^0 + a^1x + a^2x^2 + \dots + a_{t-1}x^{t-1}$ is used to generate multi-modalities encryption key (master key), such that any sub group of threshold number of valid user keys can be used to regenerate the master key. Multi-key multi-modalities biometric encryption can secure the data of businesses to be stored at cloud and fix the operation responsibility shown in figure 1.

Furthermore, it also solves the forgotten password problem of righteous users. Multi-key multi-modalities biometric encryption scheme is secure by multiple means as no single user have the complete key to unlock the data, user-keys are derived from their biometric traits those cannot be stolen or hijacked easily by the intruders. As shown in Figure 2, the multi-key multi-modalities biometric decryption process involves acquiring and preprocessing biometric modalities like fingerprints and audio from users to prepare them for feature extraction.

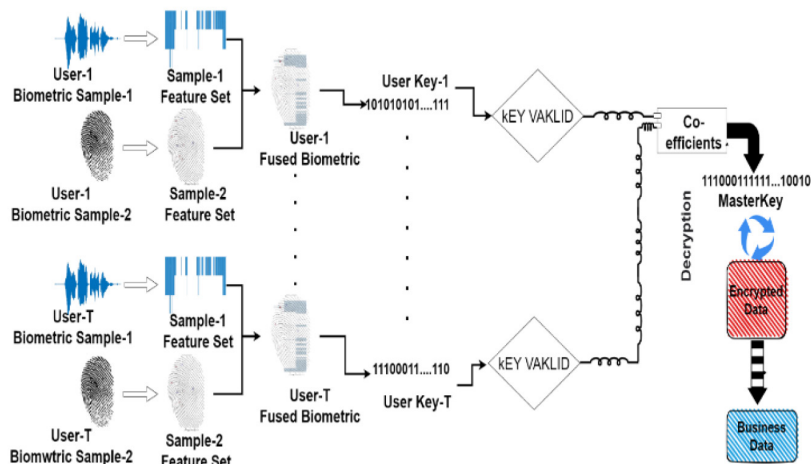


Figure 2
Multi-key multi-modalities biometric decryption

The extracted feature vectors are salted, fused, and used to derive individual user keys, which, along with Lagrange polynomial coefficients, generate a master cryptographic key. This master key is then used to decrypt the data and provide it to authorized users.

4. Experimental Results

The process used with standard fingerprint images databases FVC2002 and standard audio database cv-corpus-8.0 for the implementation and testing purpose. First Preprocessing of the biometric samples is performed to make the sample ready for feature vectors extraction.

The fingerprint images undergo pre-processing, resizing, and conversion to grayscale. The fingerprint images are first pre-processed, resized, and converted to grayscale. A 2-D Gaussian smoothing filter with a standard deviation of 0.5 is then applied to reduce noise. The images undergo histogram equalization for enhancement and are normalized within the range $[0, 1]$. Otsu's method is used to determine a global threshold that minimizes intraclass variance. Next, the images are binarized and further refined. Masks are created, and key minutiae features such as terminations, bifurcations, crossings, and dots are extracted. In the final step, any erroneous minutiae are identified and removed.

Similarly, audio samples are also pre-processed as depicted through the Figure 3, Audio is pre-processed by following the processes like Audio

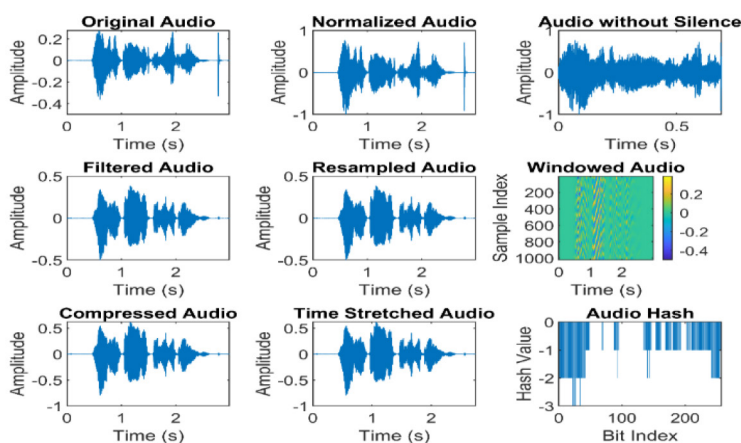


Figure 3

Audio pre-processing and features identification

normalization, Silence removal, Filtering using low pass, Resampling, Windowing using hamming window, Dynamic range compression, Time Stretching and Audio salting (further to save the keys from brute force attacks audio is salted). Mel-frequency cepstral coefficients are initially extracted from the audio input. Next, Principal Component Analysis is applied to reduce the data's dimensionality by transforming the correlated variables into a new set of uncorrelated ones, which are derived as linear combinations of the original variables.

Feature vectors are derived from the salted audio samples and identified minutiae after removal of false minutes from fingerprint are used to generate byte sequence converted to hashes using CRC-32 checksum algorithm. Feature vectors of the biometric modalities are fused using concatenation. Subsequently user keys are generated from the fused modalities.

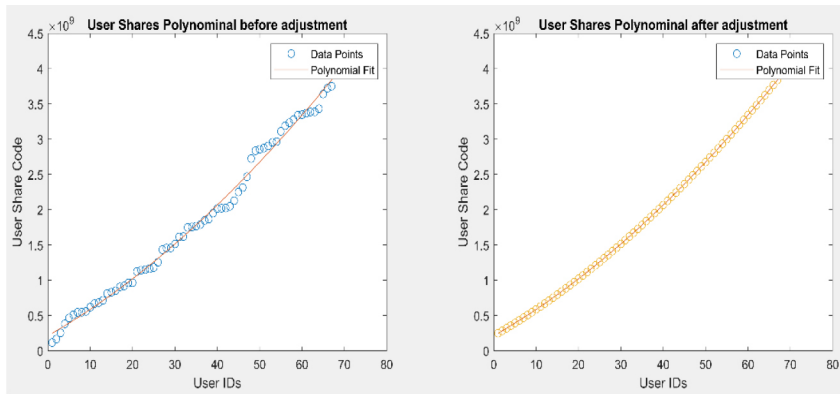


Figure 4
User keys interpolation

User keys (multi-modalities keys) are interpolated to generate the master key as per decided threshold to generate the master key (multi-key multi modalities biometric key) shown in figure 4.

$$secret = \sum_{j=1}^t y_j \cdot \prod_{\substack{i=1, \\ i \neq j}}^t \frac{x}{x_i - x_j} \pmod{p} \quad (1)$$

AES public-key cryptosystems approach is used for symmetric key encryption with generated master key. Encrypted data uploaded to cloud space for storage and later retrieval. For data retrieval, Data decryption master key is generated using polynomial basis threshold number of keys

or more keys, and data is decrypted successfully after downloading the same from cloud. further as per scheme requirement less than threshold user keys are not generating the master key. consequently, data is not decrypted with less than the threshold number of user keys.

$$\ell_{i(x)} = \prod_{j=0}^n \frac{(x - x_j)}{(x_i - x_j)} \quad (2)$$

As per the business requirement and level of data superiority this encryption scheme can be easily extended to further enhance the security of the system by checking the liveness of samples to avoid the use of stored biometric or maliciously obtained biometric samples. To further increase the system security, origin of the download data request can be verified, to ensure that business data can be accessed only from the business premises. Which in terms save the data to be accessed by the employee from outside of the business premises.

Table 1
Single vs multi-modality biometric scheme performance

Biometric Approach	FAR	FRR	GAR	GRR
Single Biometric key	5%	3%	97%	95%
Multi-Modalities Key	2%	4%	96%	98%

From table 1 its clear Multi-key multi-modalities scheme performed well compared to Uni-biometric based system. Multi-modalities scheme performed better than the single biometric schemes as expected, due to increased discrimination power generated by fusing multiple biometric traits. FAR (False Acceptance Rate) is reduced and GRR (Genuine Rejection Rate) is increased. on the other hand, there is slight increase in FRR (False Rejection Rate) and slight drop in GAR (Genuine Acceptance Rate). GAR drop can be accounted for the use of multiple modalities to be verified and due to the natural variation in biometrics. Similarity index can be reduced to improve the GAR consequently FRR will also decrease. Nevertheless, to make the system more robust, high similarity index should be used to consider the matches. The performance drop of GAR is acceptable considering the increased system security.

5. Conclusion

Cloud computing is acting as an enabler for businesses, but businesses using the cloud for data storage have good reasons to be concerned about the security of their data stored in the cloud. Some security vulnerabilities in cloud computing are inherent to the underlying technologies, while others arise due to the nature of the technology. Multi-key multi-modalities biometric encryption scheme can help all the businesses using cloud as storage for securing their data. Encrypting the data with biometric based master encryption key which can only be reproduced with threshold number of keys will prevent many issues. at the source itself, will make the data in transit and on the cloud safe from hackers and malicious cloud providers.

This scheme security comes from the fact that it hides valuable information from the hackers. Which reduces the chances to brute force the system and elevate the overall level of business data security. In future, multi-key multi-modality encryption scheme can be enhanced to work as fully homomorphic encryption scheme for cloud storage, that will reduce the cost of data change operations, as changes can be made to encrypted data without downloading the data.

References

- [1] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography algorithms for enhancing IoT Security," *Internet of Things*, vol. 22, p. 100759 (Mar. 2023), doi: 10.1016/j.iot.2023.100759.
- [2] T. Gundu, "Enhancing remote work security: a Multi-Key biometric authentication scheme for virtual workspaces," 2021 ICECET, pp. 1–7 (2023).
- [3] L. Li, H. Zhu, Y. Zheng, F. Wang, R. Lu and H. Li, "Efficient and Privacy-Preserving Fusion Based Multi-Biometric Recognition," GLOBECOM 2022 - Rio de Janeiro, Brazil, pp. 4860-4865 (2022).
- [4] C. Silva, V. A. Cunha, J. P. Barraca, and R. L. Aguiar, "Analysis of the cryptographic algorithms in IoT communications," *Information Systems sFrontiers*, vol. 26, no. 4, pp. 1243–1260 (May 2023).
- [5] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities." (2008).

- [6] C. Wang, Q. Wang, K. Ren, and W. J. Lou, "Ensuring Data Storage Security in Cloud Computing," *Iwqos: 2009 Ieee 17th International Workshop on Quality of Service*, pp. 37-45 (2009), doi: 10.1109/IWQoS.2009.5201385.
- [7] Y. Chen, V. Paxson, and R. H. Katz, "What's New About Cloud Computing Security?" University of California, Berkeley Report No. UCB/EECS-2010-5 January, vol. 20, no. 2010, pp. 1-8 (2010), doi: 10.1007/978-1-4419-6524-0.
- [8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," *Ieee Infocom*, p. 9 (2010), doi: 10.1109/INFCOM.2010.5462173.
- [9] A. Jagadeesan, T. Thillaikkarasi, and K. Duraiswamy, "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature," *Int J Comput Appl*, vol. 2, no. 6, pp. 16-26 (2010), doi: 10.5120/673-946.
- [10] S. O. Kuyoro, F. Ibikunle, and O. Awodele, "Cloud Computing Security Issues and Challenges," (2011).
- [11] B. Loganayagi and S. Sujatha, "Enhanced Cloud Security by Combining Virtualization and Policy Monitoring Techniques," *Procedia Eng*, vol. 30, no. 2011, pp. 654-661 (2012), doi: 10.1016/j.pro-eng.2012.01.911.
- [12] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583-592 (2012), doi: 10.1016/j.future.2010.12.006.
- [13] M. Borgmann, A. Rossow, M. Johns, B. Kolosnjaji, and H. Baier, On the Security of Cloud Storage Services (2012). [Online]. Available: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf
- [14] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," in *2012 International Conference on Computer Science and Electronics Engineering*, IEEE (Mar. 2012), pp. 647-651. doi: 10.1109/ICCSEE.2012.193.
- [15] S. K. Sood, "A combined approach to ensure data security in cloud computing," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1831-1838 (2012), doi: 10.1016/j.jnca.2012.07.007.
- [16] Y. Yu, L. Niu, G. Yang, Y. Mu, and W. Susilo, "On the security of auditing mechanisms for secure cloud storage," *Future Generation Computer Systems*, vol. 30, pp. 127-132 (2014), doi: 10.1016/j.future.2013.05.005.