Cloud-Based Approaches to Multi-Modal Biometric-Based Authentication in Identity Management Systems

Adedoyin Abiodun Talabi[1], Olumide Babatope Longe[2],
Muhammad Aminu Ahmad[3], Kunle Olusanya[4]
[1]*African Centre of Excellence in Technology Enhanced Learning, National Open University of Nigeria*
[2]*Faculty of Computational Sciences and Informatics, Academic City University College, Ghana*
[3]*Department of Computer Science, Kaduna State University, Nigeria*
[4]*ISACA, Ibadan, Nigeria*

Abstract

A review of cloud-based approaches to multimodal biometric identity authentication amid cyber risk management was undertaken in this research. Fifty-four (54) research works were selected out of one hundred (100) reviewed for analysis to determine biometric feature extraction means, fusion level used, and fusion strategy employed and their strengths, limitations, and accuracy performance levels. The results showed that the fingerprint was the most popular biometric used, followed by the face and iris. The weighted sum rule and matching score fusion was the highest used. Cloud-based approaches, BlockChain technologies, deep learning and Cryptography were not popular and presented research gaps for future work.

Keywords: Biometric-based Authentication, Cloud, Identity Management Systems Multi-Modal

1. Introduction

The use of the internet has grown exponentially, and many applications are now hosted and driven through the internet due to the size of the database and number of users [1]. Identity management as a gateway to applications, systems and networks has become a critical component of cybersecurity strategy in organisations and is a major tool for protecting digital information assets from hackers. Cloud storage offers a secure platform to store credentials securely for global access in a cost-effective, dynamic and scalable manner

The aim of the study is to investigate different cloud-based approaches used for multimodal biometric-based authentication in identity management systems. The objectives of this research are:

i. Identify various multimodal biometric authentication approaches used in identity management.

ii. Identify cloud-based approaches and applications used in identity management.

iii. Categorize and Analyze the different approaches derived from (i and ii) above.

iv. Establish modality, methodology, strength, weaknesses, and limitation of approach.

v. Identify trends in research approaches that can be used with minimum (FAR) and (FRR).

Research Scope - The research conducted a systematic literature review of approaches to multimodal biometric authentication in identity management used by researchers, with emphasis on cloud-based methodologies. The objective was to identify authors and year of research, biometric used, research methodology, fusion levels used and fusion strategy and/or algorithms applied. The result was then used to gauge the strength, weaknesses and limitations of the approach used. It is expected that this outcome will help other researchers when developing new approaches and techniques to build robust identity management systems using multimodal biometrics

2. Literature Review

Cybersecurity Theoretical Framework – Cyber security researchers have tried to use behavioural theories to explain behaviour and response to Cybersecurity rules by individuals generally. Lebek et al. [2] Focused on four behavioural theories: General Deterrence Theory (GDT), Technology Acceptance Model (TAM), Protection Motivation Theory (PMT) and Theory of Planned Behaviour (TPB) and present salient factors that have significant effect and influence on employee security behaviour.

All the four theories were used and combined in meta-model to explain the behavioural intention (BI) or actual behaviour (AB) of employees in relation to complying with information security measures in organizations using different causal factors. The overall goal is to raise the level of information security awareness (ISA) of members, groups and organizations and reduce the gap between behavioural

| DOI: 10.20533/ijicr.2042.4655.2022.0139

intention (BI) and actual behaviour (AB) with the specific objective to ensure compliance with information security policies and procedures.

Cybersecurity and identity Management Conceptual Framework – Cybersecurity refers to the different techniques used to protect organizational data from cyber-attacks and techniques used to prevent unauthorized access to systems, networks, applications, and devices. The consequences of cyber-attacks include loss of revenue, loss of reputation, lawsuits if clients' data are exposed and disruption of business operations. Examples of cyber-attacks include online identity theft, malware attacks, SQL injection, phishing, spoofing and cross-site scripting etc. Cybersecurity risk management involves using all available techniques and methods to ensure that only authorized users have access to organizational systems with robust identification and verification systems in place.

Overview of Biometric Systems and Types - According to Lumini and Nanni [3], Biometrics refers to the use of physical and behavioral characteristics such as fingerprints, hand geometry, face, iris etc. to identify and verify individual identities assisted by technology. Biometric applications include forensic investigation, surveillance systems, border control, access control, paternity determination, and electronic medical records management. Unimodal biometrics authentication involves the use of a single biometric trait like fingerprint while Multimodal authentication involves the use of multiple biometric traits for identifying individuals in identity systems and may include the use of fingerprint, face, palm or the iris [4].

3. Overview of Cloud Computing

According to Trader [5], using Cloud computing enables convenient, on-demand and global access to shared computing resources such as networks, servers, applications, and services. Many organizations are migrating their biometric identification management systems to cloud platforms because of faster deployment speeds, reduced investment in hardware, maintenance, software updates and applications. It enables centralized sharing of processing capabilities. Cloud-based systems can be accessed through various platforms such as mobile, access control applications and intelligence environments. Using standard governance frameworks like ISO 270001 and ISO 27002 also provides requirements for having required controls to implement security best practices.

4. Statement of the Problem

Identity management has become a critical component of cybersecurity strategy as unauthorized access to systems and networks can lead to fraud, identity theft, loss or revenue and reputation and disruption to normal operations of individuals, organizations, and government. Cyberattacks have become common with financial losses estimated in billions of US Dollars, according to the 2021 Identity Fraud Study by Javelin Strategy and Research [6]. These attacks can be from hackers, hacker groups and state-sponsored cybercriminals. Therefore, a robust identity management system for identification and authentication must be in place. Cloud-based approach to multimodal biometric based authentication have found use in this area. This paper undertakes a systematic review of existing literature in this research area to determine the extent of the use of cloud-based approaches for authentication in identity management systems.

5. Research Methodology

The paper conducted a systematic review of existing literature on the use of multi-modal biometric-based authentication in identity management systems, with emphasis on cloud-based approaches with a view to identifying the biometric trait(s) used, level of fusion, fusion strategy, and strength and limitations/research gaps. This will help to provide an overview on the popularity of cloud-based approaches in identity research works and also highlight trending research directions.

6. Research Gaps Identified

Six (6) researchers used cloud-based techniques. Two researchers (2) used IoT based techniques, 2 used BlockChain technology, 1 used QR code, 1 used deep learning approach, 1 used fuzzy logic, and 5 used cryptographic algorithms to improve their accuracy levels which provided additional security for the identity management systems. This suggests that cloud-based approaches and others listed above are research gaps that can be further explored to implement robust and secure systems. They all suggest new trends in multimodal approaches to improve current performance levels and protect individual applications, systems, networks, platforms and make the internet safe to use as we become cloud users by default due to the explosion in BIG Data usage. This will ensure meeting the information security goals of confidentiality, integrity and availability

7. Discussion and Results

The systematic literature review involved the examination and analysis of fifty – four research works that employed multimodal biometric approaches. The summary of the analyses is shown in the following Tables.

According to the results shown in Table 1, 60% of the researchers used the fingerprint biometric in their work, 48% used the face, 36% used the iris, 18% used the finger vein, 16% used the palm print, 10% used speech/voice, 4% used the finger knuckle print (FKP), 2% used age/gender features, 2% used the ear, 2% used hand geometry and 2% used the retina. This suggests that the fingerprint is the most popularly used biometric modality, followed by the face and iris.

Table 1. Biometrics Traits Usage in %

S/N	Biometric Trait	Frequency (out of 50)	%
1.	Fingerprint	30	60
2.	Face	24	48
3.	Iris	18	36
4.	Finger Vein	9	18
5.	Palm print	8	16
6.	Speech/Voice	5	10
7.	Finger Knuckle Print (FKP)	2	4
8.	Age/Gender Features	1	2
9.	Ear	1	2
10.	Hand Geometry	1	2
11.	Retina	1	2

Table 2. Different Biometric Traits combinations of used by Different Researchers in %

S/N	Biometric Combination	Count	S/N	Biometric Combination	Count
1	Face and Fingerprint	7	12	Hand and Face	2
2	Fingerprint, Iris	5	13	Fingerprint, Face ,Age and Gender Features	1
3	Palm print and Fingerprint	3	14	Fingerprint, Face and Voice	1
4	Speech and Face	2	15	Fingerprint and Speech	1
5	Iris, Fingerprint and Face	2	16	Fingerprint and Finger vein	2
6	Iris, Face, Finger Vein	2	17	Finger Knuckle Print and Iris	1
7	Left Ear, Right Ear	1	18	Finger Knuckle print and face	1
8	Iris, Retina and Finger vein	1	19	Face, Iris and Palm print	1
9	Iris, Face, Finger Vein and Palm print	1	20	Face and Iris	1
10	Iris and Voice	1	21	Hand Geometry and Palm print	1
11	Iris and Palm print	1			

Table 3. Comparative analysis of Multimodal Authentication, fusion levels and fusion strategy vis-a-vis-performance levels

	Author(s)/year	Biometric	Extraction Means	Fusion level	Fusion Strategy	Performance Achieved
1	Mwaura, Grace. (2017).	Face and Fingerprint	crossing number (CN) technique	matching score level	weighted sum rule	Accuracy of 98.67%.
2	Sharma, J and Sharma D.V (2018)	Face and Fingerprint	Minutia algorithm for finger print and MFCC for Speech	matching score	Sum rule	FAR= 0.01831, FRR= 0.00815.
3	Komal, Chander Kant (2019)	Finger Knuckle Print (FKP) and Face	AES algorithm with fingerprint based key	authentication time, decision level fusion	AND rule fused with AES algorithm	99.8%

Copyright © 2022, Infonomics Society | DOI: 10.20533/ijicr.2042.4655.2022.0139

4	Sharma Om et al (2019)	Iris and Fingerprint	Canny Edge detection and Hough transform techniques.	Matching score level	Weighted Sum-Rule	99% accuracy
5	Dhanraj et al (2021	Face And Fingerprint	SIFT and PSO for the facial category and ridges and minutiae extractions for the fingerprint	Matching score level	Summing rule	99.2%. FAR and FRR of 2% and 1.03% respectively

Table 4. Analysis of Selected Cloud – based Research Works

S/N	Author(s)/year	Title	Biometric	Methodology	Strength	Limitation
1	Sahithi S et al (2019)	Biometric Security for Cloud Data using Fingerprint and Palm Print	Fingerprint and Palm Print	Fusion of fingerprint and palm print with Advanced AES /Diffie-Helman for key exchange	Use of Cryptographic algorithm	Implementation issues
2	Selvarani P and Malarvizhi N. (2016).	Data Security in Cloud using Multi Modal Bio/cryptographic. Authentication	Iris and fingerprint	Encryption and decryption of biometric data with blowfish algorithm	Cloud storage and middleware to connect and cryptographic key. Improved speed	Security of cloud storage with password system and strength of blowfish algorithm (symmetric key used)
3	Vimal Rosy J (2020)	Biometric Security for Cloud Data Using Fingerprint.	Fingerprint and palm print	Converting fingerprint images into QR Code and encrypted with public key cryptography(AES) and stored in the cloud	Cloud storage provides anywhere access. Encryption provides security	Internet access. Image quality. Continuous and uninterrupted availability of the network
4	Farid, et al. (2021).	A Smart Biometric Identity Mgt. Framework for Personalized IoTand Cloud Computing-Based Healthcare Services	Fusion of electrocardiogram (ECG) and photoplethysmogram (PPG) signals	Internet of Things (IoT) and cloud computing-based healthcare services	use of Homomorphic Encryption (HE).	End-to-end security not yet validated Susceptible to man in the middle and replay attacks, .

Table 2 shows the different combinations of biometric traits used by different researchers. Also, all the researchers concluded that multimodal biometrics provide a higher level of accuracy than unimodal or single biometric based identity management systems as shown in Table 3. Many of the results using multimodal biometrics produced high accuracy levels. Table 4 shows the analysis of some of the research works that used cloud-based authentication techniques.

Shameem, et al. [7] used IoT technology in biometric secure authentication system. Vasavi et al. [8] used Feature-level fusion and Rivest Shamir Adleman (RSA) encryption based FEP-RSA-MM biometrics system. Alay et al [9] suggested that the fusing and use of three biometrics produced a higher accuracy than using two biometrics. It was also clear that the result depended on the strength of the algorithm used and the fusion level applied on the biometric data. Rosy [10] converted fingerprints into QR code and encrypted it with cryptographic algorithm, AES and stored in the cloud. Gayathri [11] used Grey Scale Visual Cryptography to Secure Biometric Data during Transmission and Storage in Database. Onuja AM, et al. [12], used elliptic curve cryptography (EEC) integrated with iris and voice as the multimodal biometric traits.

Mwaura [13], Sharma [14], Sharma Om et al. [16] and Dhanraj et al. [17] all used fingerprints as part of the biometric traits in their research works and fused the biometrics at matching score level using the sum rule and achieved a minimum of 98% accuracy. Komal [15] used the finger knuckle print (FKP) and face as his biometric traits and fused them at decision level combined with AES algorithm with 99.8% accuracy. This suggests that fusion at matching score level using sum rule as fusion strategy produces high level of accuracy.

Sahithi S et al. [18] fused fingerprint and palm print with Advanced AES /Diffie-Helman for key exchange, Selvarani [19] used encryption and decryption of biometric data with blowfish algorithm, Vimal [10] converted fingerprint images into QR Code and encrypted them with public key cryptography(AES) and stored in the cloud. Farid, et al. [20] fused electrocardiogram (ECG) and photoplethysmogram (PPG) signals to be used for IoT and cloud computing-based healthcare services. This research highlighted newer approaches and research gaps that can be further explored in building secure identity systems.

8. Conclusion

The conclusion is that using multiple biometrics will reduce the effects of all negative environmental factors like data quality. Cloud computing enables convenient, cost effective, on-demand and global access to shared computing resources such as networks, servers, applications, and services. Cloud platforms are deployed faster, reduced investment in hardware, maintenance, software updates and applications. Cloud deployment enables centralized sharing of processing capabilities. Using existing governance frameworks like ISO 270001 and ISO 27002 will also provide requirements for having required controls to implement security best practices. Therefore, use of cloud-based authentication techniques represents research gap that should be explored by researchers for speed of access, efficiency, cost effectiveness and scalability.

9. References

[1] Opportimes.com. (2022). the growth of the internet in the world. https://www.opportimes.com/the-growth-of-the-internet-in-the-world/#google_vignette. (Access Date: 4th January 2023).

[2] Lebek, B., Uffen, J., Neumann, M., Hohler, B., and Breitner, M. (2014). Information security awareness and behavior: A theory-based literature review. Management Research Review. 37. 1049-1092. DOI: 10.1108/MRR-04-2013-0085. (Access Date: 23 September 2021).

[3] Alessandra Lumini, Loris Nanni, (2017). Overview of the combination of biometric matchers, Information Fusion, Volume 33, Pages 71-85, ISSN 1566-2535. DOI: 10.1016/j.inffus.2016.05.003. (Access Date: 23 September 2021).

[4] R. Parkavi, K. R. Chandeesh Babu and J. A. Kumar, "Multimodal Biometrics for user authentication," (2017) 11th International Conference on Intelligent Systems and Control (ISCO), 2017, pp. 501-505, DOI: 10.1109/ISCO .2017.7856044. (Access Date: 01 November 2021).

[5] Trader. J. (2016). Benefits of cloud-based biometric identification management. https://www.m2sys.com/blog/ cloud-computing/benefits-cloud-biometric-identification-management/. (Access Date: 3rd February 2022).

[6] Businesswire.com. (2021). Total Identity Fraud Losses Soar to 56 Billion in 2020. www.businesswire.com/ news /home/20210323005370/en/Total-Identity-Fraud-Losses-S oar-to-56-Billion-in-2020. (Access Date: 01 November 2021).

[7] Shameem, Z.A., Mohite, J.N., and Sharmin, S (2017). A Review on Advance Biometric Fingerprint Based Security Systems. International Journal for Research in Applied Science and Engineering Technology (IJRASET). ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887. Volume 5 Issue X1, November 2017 (Access Date: 26 October 2021).

[8] Vasavi, K., and Latha, Y. (2019). RSA Cryptography based Multi-Modal Biometric Identification System for High-Security Application. International Journal of Intelligent Engineering and Systems. 12. 10-21. DOI: 10.22266/ijies2019.0228.02. (Access Date: 01 November 2021).

[9] Alay, N., and Al-Baity, H. (2020). Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits. Sensors. 20. DOI: 10.3390/s20195523. (Access Date: 03 November 2021).

[10] Vimal Rosy, J. (2020). Biometric Security for Cloud Data Using Fingerprint. Science, Technology and Development. Volume IX Issue II FEBRUARY 2020. ISSN: 0950-0707. (Access Date: 31 October 2021).

[11] Gayathri, M., and Malathy, C. (2020). A Technique to Secure Multimodal Biometric Data Using Visual Secret Scheme. International Journal of Advanced Science and Technology, 29(06), 2406 - 2417. (Access Date: 01 November 2021).

[12] Onuja, A. M., Oyefolahan, I. O., Adebayo, O. S., Isah, A. O., Olaniyi, M., et al. (2021) Secured E-Commerce System using ECC and Multimodal Biometrics. Am J Computer Science Information Technology Vol. 9 No. 8: 103. (Access Date: 01 November 2021).

[13] Mwaura, G. (2017). Multimodal Biometric System: - Fusion of Face and Fingerprint Biometrics at Match Score Fusion Level. International Journal of Scientific and Technology Research. 6. 41 (Access Date: 26 October 2021).

[14] Sharma, J., and Sharma, D.V. (2018). Multimodal Biometric Authentication System Using Face and Fingerprint Biometric. IOSR Journal of Engineering (IOSRJEN) www.iosrjen.org ISSN (e): 2250-3021, ISSN (p): 2278-8719 Vol. 08, Issue 4 (April. 2018), ||VI|| PP 54-62. (Access Date: 01 November 2021).

[15] Komal, C. Kant. (2019). A Robust Multimodel Biometric Crypto System. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2S8, August 2019. (Access Date: 04 November 2021).

[16] Sharma O. P., and Sivaramkumar P. (2019). An Improved Multi-Biometric System for Authentication. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019. (Access Date: 02 November 2021).

[17] Dhanraj M., Pawara, K. R. D., Gosavic, V. R. (2021). An Optimize Multimodal Biometric Authentication System for Low Classification Error Rates Using Face and Fingerprint. International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS 2021). (Access Date: 04 November 2021).

[18] Sahithi S, Anirudh A, Swaroop, Ramya, Ruth K. (2019). Biometric Security for Cloud Data using Fingerprint and Palm Print. International Journal of Innovative Technology and Exploring Engineering (IJITEE). ISSN: 2278-3075, Volume-8, Issue-6S3 (Access Date: 3 February 2022).

[19] Selvarani P., and Malarvizhi, N. (2016). Data Security in Cloud using Multi Modal Bio-cryptographic Authentication. ISSN (Print): 0974-6846.ISSN (Online): 0974-5645. Indian Journal of Science and Technology, Vol 9(34), DOI: 10.17485/ijst/2016/v9i34/86374, September 2016. (Access Date: 3 February 2022).

[20] Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., Gide, E. (2021). A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services. Sensors. https://doi.org/10.3390 /s21020552 (Access Date: 3 February 2022).