iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XI **Month of publication:** November 2024

DOI: https://doi.org/10.22214/ijraset.2024.65520

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XI Nov 2024- Available at www.ijraset.com

The Role of Biometric and Authentication in Security

Prof. Sanghesh B. Bele[1], Gokul S. Band[2], Shravan S. Kawade[3], Akash D. Udimkar[4], Rahul N. Khandare[5]
[1]*Assistant Professor, Department of MCA Vidya Bharti Mahavidyalaya, Amravati, 444602 India*
[2, 3, 4, 5]*Postgraduate student of Vidya Bharati Mahavidyalaya, Amravati, 444602 India*

Abstract: ***Biometric authentication is a user identification and authentication method utilizing unique physical or behavioral traits such as fingerprints, facial patterns, iris scans, and voice recognition. This paper explores the advantages of biometric systems over traditional methods like passwords and PINs, highlighting their resilience against replication and theft. We delve into various types of biometric systems, their strengths and weaknesses, and address key research issues that must be resolved for effective deployment in real-world scenarios. We conclude by emphasizing the potential of biometric authentication as a secure and convenient identification solution across various applications.***
Keywords: Biometric authentication, identification, security, user authentication, behavioral traits.

I. INTRODUCTION

This paper presents an imperial study on the convolutional layer in CNNs, focusing on its architecture, functionality, and applications in data mining As technology continues to evolve at an unprecedented pace, the number of technology users—and consequently the volume of data generated—has surged. Among this data, sensitive information often requires stringent protection to prevent unauthorized access. While traditional authentication methods, such as passwords, PINs, and smart cards, have long been employed to secure data, they are increasingly deemed inadequate due to their vulnerabilities. Passwords can be easily forgotten or compromised, and physical tokens can be lost or stolen.

In response to these challenges, the field of cybersecurity has shifted toward biometric authentication, leveraging unique human physiological and behavioral traits for secure identification. Biometric systems capitalize on the distinctiveness of characteristics such as fingerprints, facial features, iris patterns, and even behavioral patterns like voice and gait. These traits offer a promising alternative, as they cannot be easily replicated or forgotten, thus enhancing security while streamlining user experience.

Despite the advantages of biometric systems, concerns remain regarding their implementation and potential weaknesses. The security landscape is further complicated by the rise of digital rights management (DRM) systems, which protect digital media from unauthorized copying and distribution. Effective user authentication is critical in these systems, where the authenticity of access rights must be confirmed.

Biometric technology has witnessed significant advancement since the introduction of the first commercial device over 25 years ago. Today, a variety of biometric modalities are employed across diverse applications—from securing smartphones and ATMs to enhancing surveillance systems and controlling access to sensitive facilities.

This paper aims to explore the landscape of biometric authentication, comparing various methods and assessing their effectiveness, user acceptance, and the challenges they present. By conducting a survey of 99 users, we will analyze preferences and perceptions regarding biometric systems, ultimately highlighting the critical role of these technologies in modern information security.



Type of Biometrics System.

©IJRASET: All Rights are Reserved

II. LITERATURE REVIEW

Biometric authentication, a method of identifying individuals based on unique physical or behavioral traits, has emerged as a powerful security tool. Its significance lies in its ability to offer high levels of security, convenience, and precision, making it an increasingly popular solution across various industries.

Sr. No	Author Name	Conclusion	Source	Year
i.	Rebin Abdulkareem Hamaamin	Biometric identification systems offer secure and efficient access control, improving accuracy and convenience over traditional methods. Despite challenges like privacy concerns, continued advancements will enhance their effectiveness and security. 4o mini	Research Gate[1]	2024
ii.	Elvir Misini	Biometric authentication offers a more secure alternative to traditional passwords, but it also has weaknesses, including the potential for theft or forgery. Combining biometrics with multi-factor authentication can provide enhanced security for protecting sensitive data.	Research Gate[2]	2022
iii.	Arun Ross	Biometric systems enhance security but face challenges in privacy, cultural resistance, and integration, requiring balanced solutions for effective adoption.	Research Gate[3]	2006
iv.	Vinayak Pujari	Advances in biometric technology have made it secure, cost-effective, and efficient, with improved performance in various identification methods.	Research Gate[4]	2021
v.	Mymoon Dobaibi	The study found that age and education significantly influence user acceptance of biometric systems, with fingerprint authentication being the most preferred and perceived as secure by the majority of participants.	Diva Portal[5]	2023
vi.	Rahul Ranjan	Biometric authentication offers strong security but requires careful system design and legal frameworks to address privacy risks and ensure proper protection of biometric data.	Research Gate[6]	2009
vii.	Hussaini Mamman	Biometric authentication methods, like fingerprint and password techniques, offer effective security, but future work should explore both simple and complex methods for enhanced understanding and improvement.	Research Gate[7]	2020
viii.	Gurudatt Anil Kulkarni	Biometrics offers secure, reliable identification by analyzing physical and behavioral traits, with multimodal systems enhancing security and convenience across various applications.	Research Gate[8]	2012
ix.	Preeti Sharma	Biometrics and machine learning offer vast potential across industries but must be implemented ethically, addressing privacy, accuracy, and bias concerns.	Research Gate[9]	2023
x.	Israa Alsaadi	Biometric security methods, especially when combined (e.g., fingerprint, iris, and face recognition), offer improved reliability, accuracy, and flexibility for securing sensitive systems.	Research Gate [10]	2015
xi.	ZHANGRUI	This paper reviews biometric authentication advancements, categorizing systems into static and dynamic features, while emphasizing the need for improved security and privacy in future research.	IEEE[11]	2017
xii.	Prashant Shrivastava	Biometric authentication provides enhanced security for critical applications and, with future advancements like DNA matching and combined systems, promises even greater protection.	Research Gate[12]	2016
xiii.	U. SUMALATHA.	Multimodal fingerprint biometrics offer improved accuracy and security over unimodal systems, but further advancements in sensors, algorithms, and privacy measures are needed for reliable, user-friendly solutions.	IEEE[13]	2024
xiv.	JAMMI ASHOK	Biometrics, replacing traditional authentication methods, is evolving alongside nanotechnology to create ultra-small, secure systems with the potential to store vast personal data.	Research Gate[14]	2010
xv.	Marc Pasquet	Biometric authentication, including multimodal systems, is evolving to enhance security in applications like e-transactions, with potential future innovations such as biometric payment methods and devices.	Research Gate[15]	2008
xvi.	AMARPREET SINGH	Biometric systems, while effective for personal recognition and security, must be combined with other technologies and carefully designed to balance security, privacy,	Research Gate[16]	2010

III. CONCLUSIONS

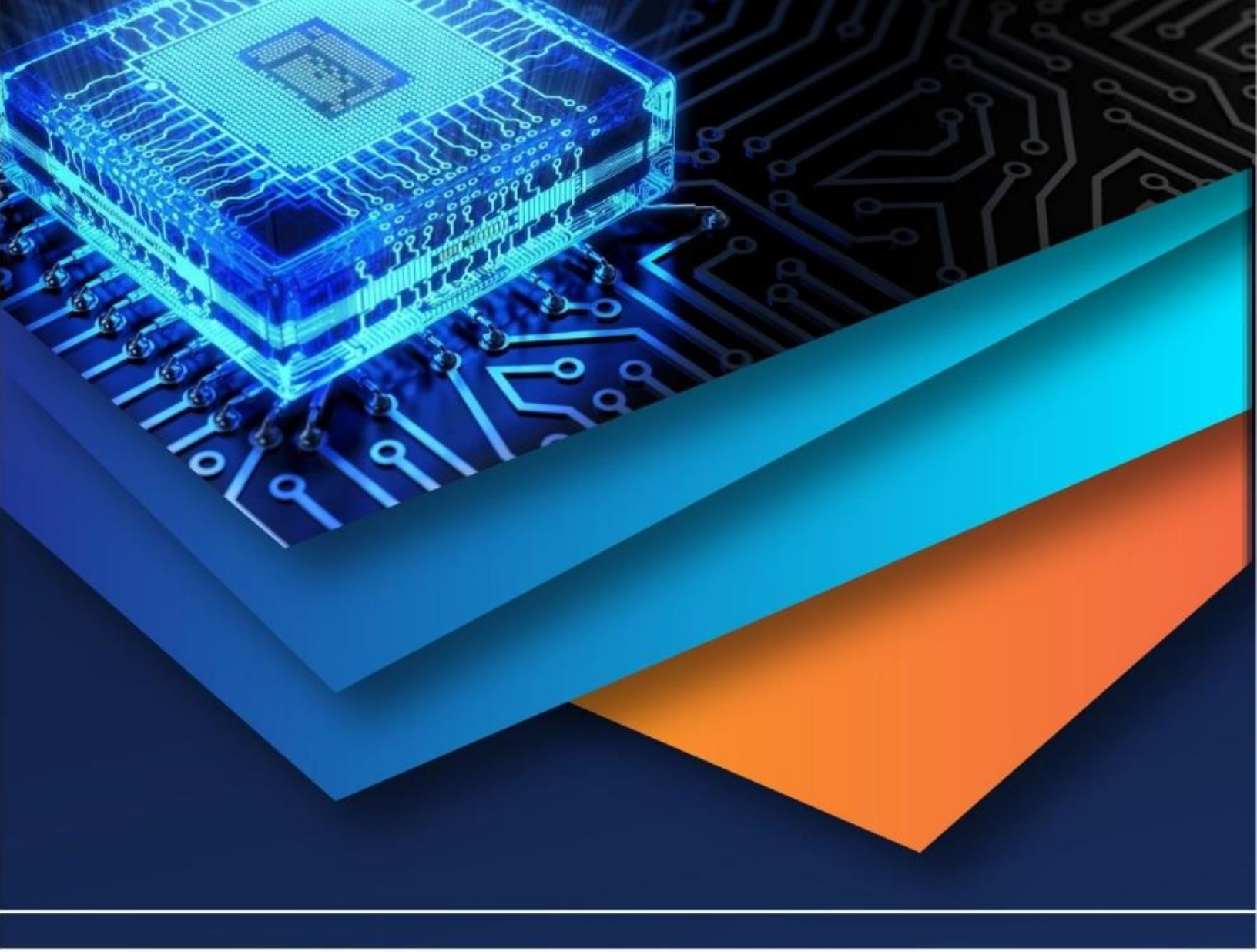
Biometric identification is growing in usage for physical and virtual access control, with advancements like digital imprints, face recognition, and voice verification replacing traditional methods. This paper discusses match-in database biometric technology, identifies current threats, and suggests a more comprehensive threat model. Decentralized databases can enhance security and privacy in biometric authentication systems.

Dynamic biometric devices need higher accuracy and data fusion can improve authentication accuracy. Biometrics are crucial for reliable personal recognition, but a combination of biometric and non-biometric elements is needed for robust system design. Biometrics have potential in secure applications like e-Commerce, access control, and e-Banking, with the future evolution and embedding of biometric technology influencing daily business operations.

REFERENCES

[1] R. Kannavara and N. Bourbakis, ‘‘A comparative survey on biometric identity authentication techniques based on neural networks,’’ in Biometrics: Theory, Methods, and Applications, N. V. Boulgouris, K. N. Plataniotis, and E. Micheli-Tzanakou, Ed. 2009, ch. 3, pp. 47–79.
[2] S. Shunmugam and R. Selvakumar, ‘‘Electronic transaction authentication—A survey on multimodal biometrics,’’ in Proc. IEEE Int. Conf. Comput. Intell. Comput. Res., Dec. 2014., pp. 1–4.
[3] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, ‘‘Surveying the development of biometric user authentication on mobile phones,’’ IEEE Commun. Surveys Tuts., vol. 17, no. 3, p. 1268–1293, 3rd Quart., 2015.
[4] “A Survey of Biometrics Security System”,Mohammed Nasir Uddin, Selina Sharmin, Abu Hasnat Shohel Ahmed and Emrul Hasan,Shahadot Hossain5 and Muniruzzaman, IJCSNS International Journal of Computer Science and Network 16 Security, VOL.11 No.10, October 2011.
[5] “Biometrics: An Overview of the Technology, Issues and Applications”, S. Asha, C. Chellappan, Department of Computer Science & Engineering Anna University, Chennai , International Journal of Computer Applications (0975 – 8887) Volume 39– No.10, February 2012
[6] “Analysis of various Biometric Techniques”, Mr. Sanjay Kumar, Dr. Ekta Walia, Department of Computer Science & Engineering, Maharishi Markandeshwar University, International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1595-1597
[7] “Analysis of various Biometric Techniques”, Mr. Sanjay Kumar, Dr. Ekta Walia, Department of Computer Science & Engineering, Maharishi Markandeshwar University, International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1595-1597
[8] “BIOMETRIC: CASE STUDY” Sushma Jaiswal Lecturer, S.O.S. in Computer Science, Dr. Sarita Singh Bhadauria Professor & Head, Department of Electronics Engineering Journal of Global Research in Computer Science Volume 2, No. 10, October 2011
[9] “ BIOMETRICS BASED IDENTIFICATION TECHNIQUES (BIT)”, Akash Srivastva, Vedpal Singh, CSE Dept. Dev Bhoomi Institute of Technology (DBIT), Journal of Global
[10] Research in Computer Science, Volume 2, No. 11, November 2011
[11] J. Galka, M. Masior, and M. Salasa, ‘‘Voice authentication embedded solution for secured access control,’’ IEEE Trans. Consum. Electron., vol. 60, no. 4, pp. 653–661, Nov. 2014.
[12] H. Saevanee and P. Bhattarakosol, ‘‘Authenticating user using keystroke dynamics and finger pressure,’’ in Proc. 6th IEEE Consumer Commun. Netw. Conf., Jan. 2009, pp. 1–2.
[13] M. Antal and L. Z. Szabó, ‘‘An evaluation of one-class and two-class classification algorithms for keystroke dynamics authentication on mobile devices,’’ in Proc. 20th Int. Conf. Control Syst. Comput. Sci., May 2015, pp. 343–350.
[14] K. El-Maleh and W. El-Hajj, ‘‘Voice biometrics: Security, forensics, and healthcare,’’ J. Med. Syst., vol. 43, no. 9, p. 306, 2019.
[15] K. Banerjee, J. P. Singh, and R. Kaur, ‘‘Human retinal identification: Review and future scope,’’ J. Comput. Sci. Technol., vol. 15, no. 1, pp. 10–15, 2014.
[16] I. Bouchrika, ‘‘A survey of using biometrics for smart visual surveillance: Gait recognition,’’ in Surveillance in Action: Technologies for Civilian, Military and Cyber Surveillance, 2018, pp. 3–23.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)