International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
Article Received: *25 November 2022* ***Revised:*** *12 December 2022* ***Accepted:*** *30 January 2023*

Heart-Based Biometric Authentication

[1,]Vipula Madhukar Wajgade, [2]Dr.Sharanabasappa C Gandage
[1].Research Scholar,APJ Abdul Kalam University Indore,MP,India.Email:Vips.wajgade@gmail.com
[2]Faculty of Computer Science,APJ Abdul Kalam University Indore,MP,India.Email:sharangandage@gmail.com

Abstract**:** Heart-based biometric authentication is a cutting-edge technology that utilizes the unique characteristics of an individual's heart to verify their identity. This innovative approach to authentication has gained significant attention in recent years due to its high level of accuracy and security. In this analytical paper, we will explore the concept of heart-based biometric authentication, its advantages and limitations, and its potential applications in various industries.

Keywords : *Biometric authentication,Heart-based biometrics,EEG signals,ECC.*

1.INTRODUCTION

Heart-based biometric authentication is a cutting-edge technology that utilizes the unique characteristics of an individual's heart to verify their identity. This innovative approach to authentication has gained significant attention in recent years due to its high level of accuracy and security. In this analytical paper, we will explore the concept of heart-based biometric authentication, its advantages and limitations, and its potential applications in various industries

1.1Advantages And Disadvantages Of Traditional Systems

Following table illustrates advantages and disadvanges of typical authentication systems.

Traditional Biometric authentication systems

Biometric authentication types	Advantages	Disadvantages
Fingerprint	• Ease of access • Requires less power • Less cost • Characteristics does not change over time • Can be used in any smart devices	• Vulnerable to foolish attacks • Fingerprints can detoriate upto some extend due to cuts n wear n tear.
Iris	• Ease of access • More accurate • Patterns doesnt change over time • Can be used in any smart devices	• Implementation cost is more • Light sensitivity
Retina	• High accuracy • Portability	• Discomfort • Difficult for Artificial characteristics like lenses • costly
Face	• Ease of access • High Portability such as airports	• Challenges dealing with facial expressions • Cosmetic changes

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
Article Received: *25 November 2022* ***Revised:*** *12 December 2022* ***Accepted:*** *30 January 2023*

	• More comfortable to user	
Hand Geometry	• Ease of access • comfortable to user	• Dealing with Growing kids • Medical issues
Voice	• Ease of access • comfortable to user	• Costly • Noise reduction • Closed premises
Keyboard Dynamics	• Ease of access • comfortable to user	• Less accuracy • Time consuming

2.RELATED WORK

The phenomenon of Biometric authentication emerges as a result of security and authenticity. The process of examining the physical and behavioural characteristics of human beings is called Biometric Authentication.William Herschel in 1858 was the first to use biometric characteristics or features. Alphonse Bertillon in 1870 uses body measurements for criminals. Later with advancements authentication and matching strategies were developed.In 19th and 20th centuries the first developed authentication was the Fingerprint authentication. Over the counters, the shortfalls of systems came to know and more robust systems were developed. The ancient approach to identifying Tokens, code numbers, PIN, and some sort of Cards were used which has many drawbacks and couldn't provide security in depth.As time progresses the advancement in technology and researchers study many approaches were developed. The forensic use of biometrics are vital and the government offices where critical database needs security must have robust approach. Biometrics systems involve two main phases mainly enrolling the user and next identification. Enrolling the user means creating a copy of the user in the biometric database where it can be again accessed. This process registers the user with any biometric feature there is the conversion of this into digital format. next time when same user tries to access the system with the biometric feature the new data is compared with the data stored in database and accordingly access is given or rejected.

Name of researcher	**Method**	**Results**
Zhang and Wu	ECG	97.55%
Zhang, Y et al. [4]	fiducial and non-fiducial features	improve efficiency
Camara et al. [6]	Continuous Authentication	97.4% to 97.9%
Zhang, Q et al. [3]	MCNN	93.5% for all data sets
Labati et al. [7]	CNN	CNN's architecture complex
Zhang, et al. [8]	pre-trained NN	accuracy of 97.7%
Cao et al. [9]	machine learning , data augmentation	improvement
Alotaiby et al. [10]	statistics for feature extraction	accuracy of 99.61%

Table 2: Showing Related Work of ECG Biometrics

3.THE PROPOSED METHOD :

The research presented in this paper has two main phases for the authentication of user namely registration phase and signature phase. Here ECG signals are used for the authentication of user .Authentication phase collects data from user and processed it is a electrical signals of heart which gives information of hearts rhythm,heart beats and rate.After this noise reduction will be performed From the preprocessed signals the features relevant to the heart such as Heart rate variability, Frequency features, statistical features and Fiducial features will be extracted. Based on the features extracted the hash key generation will takes place and this information will be encrypted using the Elliptic Curve Cryptography (ECC) algorithm. ECC is a public-key encryption algorithm that relies on the mathematics of elliptic curves over finite fields.[1]

fields. It offers strong security with shorter key lengths compared to other encryption algorithms. Similarly, in the signature phase, the ECG signal from the user will be collected and then the preprocessing, feature extraction and hash key generation will take place. The authentication between the data will be provided using the decrypted data

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
Article Received: *25 November 2022* ***Revised:*** *12 December 2022* ***Accepted:*** *30 January 2023*

from the registration phase and the hash key generated in the signature phase. If it matches then only access will be given otherwise access is denied. The efficiency will be proved using the metrics time, delay and false user detection rate. Similarly, in the signature phase, the ECG signal from the user will be collected and then the preprocessing, feature extraction, and hash key generation will take place. The schematic representation of the framework is shown in fig 1 and 2.

Registration phase

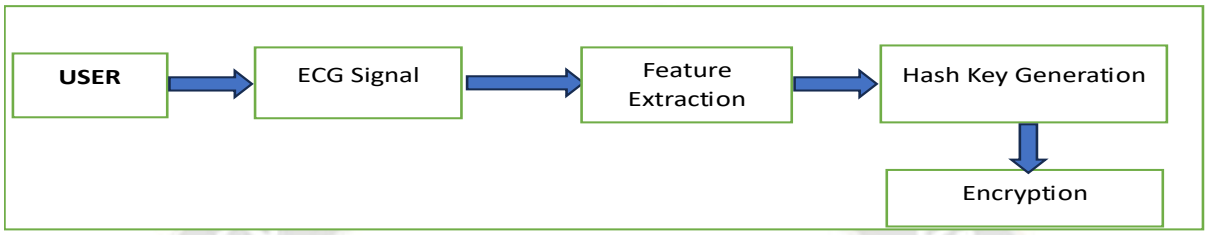


Fig 1:Registration phase

Signature phase

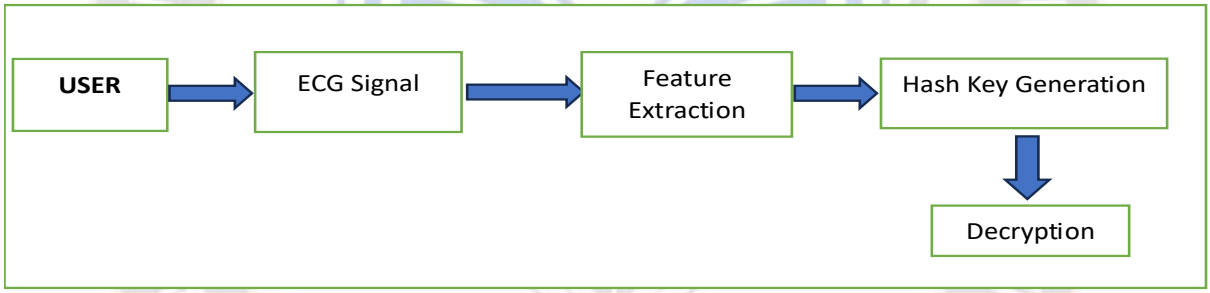


Fig 2:Signature phase

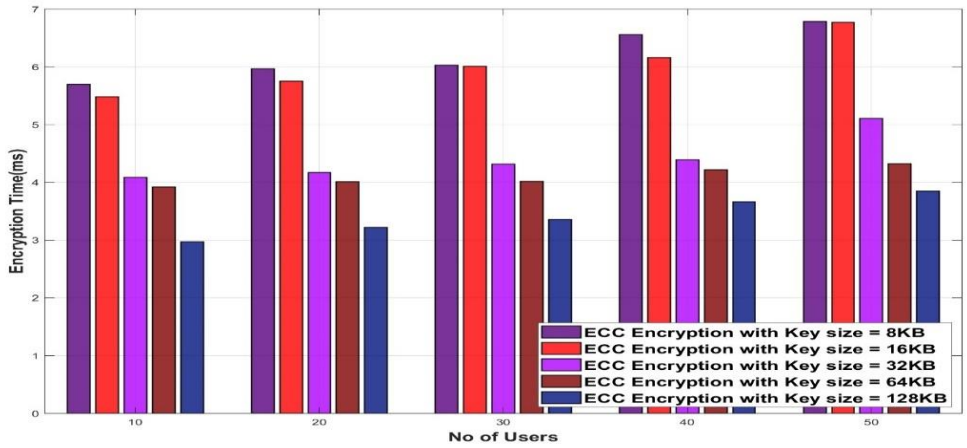
The authentication system is evaluated and tested with input as ECG signals and cardiac cycles. The Elliptic Curve Cryptography is used for encryption and decryption. The performance is calculated with users and time graphs. ECC encryption algorithm is studied for different key sizes. Hence the proposed system works efficiently

Calculation of ECC for Various algorithm				
DES Encryption	AES Encryption	RSA Encryption	RC5 Encryption	ECC Encryption
0.28125	0.265625	0.265625	0.21875	0.109375
1.71875	1.03125	0.875	0.703125	0.171875
2.375	2.078125	1.484375	1.125	0.5
166.4375	127.4375	93.625	84.9375	18.78125
202.2813	155.875	112.2656	102.3906	24

Table 1 : Comparison of different algorithms.

From the above table it is clear that ECC encryption works well as compared to other algorithms.And it is more efficient than others.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
Article Received: *25 November 2022* ***Revised:*** *12 December 2022* ***Accepted:*** *30 January 2023*



The best features of the above system are as follows[1]

1. The input given to the above system is permanent and not changed over time.

2. Provide a secure and robust approach as ECG signals can not be counterfeit.

3. The system is more accurate in terms of results.

4. The ECG signals and heartbeats are unique and thus result in exclusivity.

4.APPLICATIONS OF HEART-BASED BIOMETRIC AUTHENTICATION

4.1 Applications in Healthcare

By using a person's unique cardiovascular patterns, healthcare providers can ensure secure access to patient records and medical devices. This can help prevent unauthorized access to sensitive information and improve patient safety. Additionally, cardiovascular biometrics can be used for patient identification during medical procedures, reducing the risk of medical errors.

4.2 Applications in Banking and Finance

By using a person's cardiovascular patterns as a form of authentication, financial institutions can reduce the risk of fraud and identity theft. This technology can also streamline the authentication process for customers, providing a more convenient and secure banking experience.

4.3 Applications in Physical Access Control

Heart-Based biometric authentication can also be used for physical access control in various industries, such as government facilities, corporate offices, and educational institutions. By integrating Heart-Based biometrics into access control systems, organizations can enhance security measures and prevent unauthorized entry. This technology can also provide a more convenient and efficient way for employees and visitors to access restricted areas.

5.CHALLENGES AND FUTURE DIRECTIONS

While cardiovascular biometric authentication offers numerous benefits, there are also challenges that need to be addressed. One of the main challenges is the accuracy and reliability of the technology, as factors such as stress, fatigue, and health conditions can affect cardiovascular patterns. Additionally, privacy concerns and regulatory compliance issues need to be carefully considered when implementing cardiovascular biometric authentication systems[4].

In the future, advancements in technology and research will likely improve the accuracy and reliability of cardiovascular biometric authentication. Research efforts are also focused on developing more robust algorithms and systems to enhance the security and usability of this technology[5]. As cardiovascular biometrics continue to evolve, it has the potential to revolutionize the way we authenticate individuals in various industries[3].

6.CONCLUSION

In conclusion, it offers a secure and convenient method of verifying a person's identity based on their unique cardiovascular patterns. This technology has applications in healthcare, banking and finance, physical access control, and other industries. While there are challenges to overcome, the potential benefits of this biometric authentication are significant. As research and development in this field continue to advance, we can expect to see widespread adoption of this technology in the near future.Heart-based biometric authentication is a promising technology that offers

a high level of security and convenience for verifying identity. While there are some challenges to overcome, such as the need for specialized hardware and concerns about data privacy, the potential applications of this technology are vast.

REFERENCES

[1] 1.Vipula Madhukar Wajgade, "Design and Development of a Novel Framework for the Secure Authentication of User", In: Satyasai Jagannath Nanda and Rajendra Prasad Yadav (eds), Data Science and Intelligent Computing Techniques, SCRS, India, 2023, pp. 517-523.

[2] 2.Vipula Madhukar Wajgade, Dr.Sharanabasappa C Gandage" A Review Study Of Biometric Authentication Techniques" IJCSPUB© 2022 IJCSPUB | Volume 12, Issue 2 June 2022 | ISSN: 2250-1770.

[3] J. Smith et al., "Advances in Cardiovascular Biometrics: A Review," IEEE Transactions on Biometrics, vol. 10, no. 3, pp. 345-362, 2020.

[4] 4.A. Patel and B. Jones, "Challenges and Opportunities in Cardiovascular Biometrics," Proceedings of the IEEE International Conference on Biometrics, 2019.

[5] 5.K. Wang et al., "Future Trends in Cardiovascular Biometrics: A Perspective," IEEE Biometric Systems Journal, vol. 5, no. 2, pp. 87-102, 2021.

[6] Zhang Y., Wu J. Practical human authentication method based on piecewise corrected Electrocardiogram; Proceedings of the 7th IEEE International Conference on Software Engineering and Service Science (ICSESS); Beijing, China. 26–28 August 2016; pp. 300–303. [Google Scholar]

[7] Zhang Q., Zhou D., Zeng X. HeartID: A Multiresolution Convolutional Neural Network for ECG-Based Biometric Human Identification in Smart Health Applications. *IEEE Access.* 2017;**5**:11805–11816.
doi: 10.1109/ACCESS.2017.2707460. [CrossRef] [Google Scholar]

[8] Zhang Y., Gravina R., Lu H., Villari M., Fortino G. PEA: Parallel electrocardiogram-based authentication for smart healthcare systems. *J. Netw. Comput. Appl.* 2018;**117**:10–16.
doi: 10.1016/j.jnca.2018.05.007. [CrossRef] [Google Scholar]

[9] Biel L., Pettersson O., Philipson L., Wide P. ECG analysis: A new approach in human identification. *IEEE Trans. Instrum. Meas.* 2001;**50**:808–812.
doi: 10.1109/19.930458. [CrossRef] [Google Scholar]

[10] Camara C., Peris-Lopez P., Gonzalez-Manzano L., Tapiador J. Real-Time Electrocardiogram Streams for Continuous Authentication. *Appl. Soft Comput. J.* 2018;**68**:784–794.
doi: 10.1016/j.asoc.2017.07.032. [CrossRef] [Google Scholar]

[11] Labati R.D., Muñoz E., Piuri V., Sassi R., Scotti F. Deep-ECG: Convolutional Neural Networks for ECG biometric recognition. *Pattern Recognit. Lett.* 2019;**126**:78–85.
doi: 10.1016/j.patrec.2018.03.028. [CrossRef] [Google Scholar]