JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Internet of Things (IoT) and Biometrics: A Secure Future for Connected Devices

[1] **Dr. Haridas Janardhan Kharat,**
[2] **Dr. Prafullkumar Ashokrao Ghuge,**
Shankarlal Khandelwal Arts, Science and Commerce College, Akola, Maharashtra, India

Abstract— The Internet of Things (IoT) is rapidly transforming the world, connecting everyday objects to the internet and enabling them to collect and share data. Biometrics, the use of unique biological characteristics for identification and authentication, offers a promising solution to enhance security in this ever-growing network. Present study explores the convergence of IoT and biometrics, analyzing its potential benefits, challenges, and future directions for secure and user-friendly interaction with connected devices.

Keywords— IoT, Authentication, Recognition

I. Introduction

Recently, the explosive growth of IoT devices presents both immense opportunities and significant security concerns. Traditional password-based authentication can be vulnerable to hacking and unauthorized access. Biometrics offers a more secure and convenient approach for user verification in the context of IoT. Present investigation will delve into the integration of these technologies, exploring various biometric modalities and their applications in securing the IoT ecosystem [1].

II. Biometric Technologies for IoT:

Existing Technologies for IoT are as ..

- Fingerprint Recognition: This popular method utilizes unique fingerprint patterns for user identification. However, sensor size and cost considerations need to be addressed for widespread IoT implementation [1][2].
- Facial Recognition: Advancements in facial recognition technology offer promising solutions, but concerns regarding privacy and data security require careful consideration [2][3].
- Iris Recognition: Iris patterns provide a highly accurate and reliable identification method, but specialized sensors might not be suitable for all IoT applications [2][3].
- Voice Recognition: Voice biometrics leverage vocal characteristics for user authentication. However, background noise and voice variations can pose challenges in some environments [2] [3].

III Benefits of Biometric Authentication in IoT:

Biometric Authentication gives many benefits in IoT as..

- Enhanced Security: Biometrics offer a stronger layer of authentication compared to traditional passwords, reducing the risk of unauthorized access to connected devices and sensitive data [3].
- Improved User Convenience: Biometric authentication eliminates the need for remembering complex passwords, offering a more seamless user experience.
- Scalability and Remote Access: Biometric systems can be integrated with various IoT devices, facilitating secure remote access and control [4].

IV Challenges and Considerations:

Challenges in Biometric Authentication are as…

- Privacy Concerns: Biometric data is highly sensitive and requires robust security measures to prevent misuse and identity theft. Regulations like GDPR and CCPA need to be carefully considered when deploying biometric solutions.

- Sensor Limitations: Some biometric modalities might require specialized sensors that can be bulky or expensive for certain IoT devices. Miniaturization and cost-effectiveness remain critical areas for development.
- System Interoperability: Standardization across different biometric systems and IoT platforms is essential for seamless integration and interoperability.
- Vulnerability to Spoofing: Spoofing attacks, where fake biometric data is used to gain access, pose a potential risk. Liveness detection techniques can help mitigate this threat[4].

V FUTURE DIRECTIONS:

- Multimodal Authentication: Combining different biometric modalities can enhance security and address limitations of individual methods.
- Advanced Machine Learning: Machine learning algorithms can be utilized for continuous improvement in biometric recognition accuracy and liveness detection.
- Blockchain Integration: Blockchain technology can ensure secure storage and management of biometric data, addressing privacy concerns[5].

VI CONCLUSION:

- Present investigation reveals that the convergence of IoT and biometrics holds immense potential for creating a more secure and user-friendly connected world. By addressing the challenges and implementing robust security protocols, this integration can pave the way for a trusted and secure future for the Internet of Things.

VIII FURTHER RESEARCH AREAS

- The ethical considerations and potential biases in biometric technology.
- The impact of artificial intelligence on the development of next-generation biometric solutions.
- Standardization efforts and regulatory frameworks for secure and responsible deployment of biometric authentication in IoT.

REFERENCES

[1] Karie, N.M.; Sahri, N.M.; Haskell-Dowland, P. “IoT threat detection advances, challenges and future directions”. In Proceedings of the 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT), Sydney, NSW, Australia, 21–21 April 2020;pp. 22–29.

[2] Deogirikar, J.; Vidhate, “A. Security attacks in IoT: A survey”. In Proceedings of the 2017 International Conference on I-SMAC (IoTin Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 32–37.

[3] Gurunath, R.; Agarwal, M.; Nandi, A.; Samanta, D. “An overview: Security issue in IoT network”. In Proceedings of the 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Tirunelveli, India, 29–30 October 2020; pp. 104–107.

[4] Yang,W.;Wang, S.; Hu, J.; Ibrahim, A.; Zheng, G.; Macedo, M.; Johnstone, M.; Valli, C. “A Cancelable Iris- and Steganography-based User Authentication System for the Internet of Things”. Sensors 2019, 19, 2985.

[5] Cherapau, I.; Muslukhov, I.; Asanka, N.; Beznosov, K. On the “Impact of Touch ID on iPhone Passcodes. In Proceedings of the Eleventh Symposium On Usable Privacy and Security”, Pittsburgh, Pennsylvania, 20–22 July 2011; pp. 257–276.