IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

Fingerprint Biometric for Internet of Things

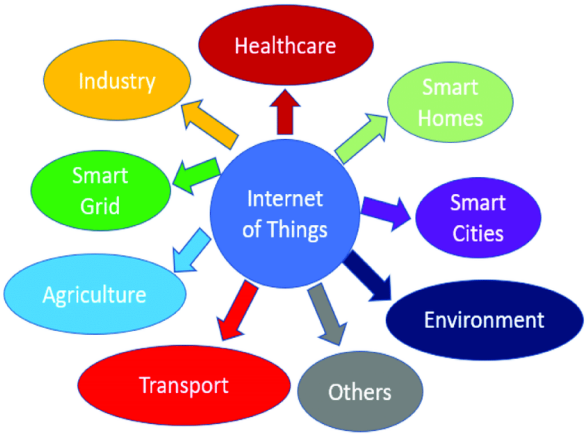
Jyotsna Nalawade
Student, Department of MCA
Late Bhausaheb Hiray S.S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *IoT security is crucial, because the larger number of Internet-of-Things (IoT) devices that require interaction between smart devices and customers. Biometrics presents an intriguing window of opportunity for improving IoT usability and security, and can play a critical role in securing a wide range of developing IoT devices to address security challenges. The goal of this study is to provide a complete overview of current biometrics research in IoT security, with a particular focus on authentication.*

Keywords: Biometrics, Fingerprint, Iot, Security, Authentication

I. INTRODUCTION

The Internet of Things (IoT) contains a variety of devices, such as wearable devices, smartphones, computers, personal digital assistants (PDAs), and tablets. These devices, which consist of embedded sensors and processors that can handle their internal states or the external environment around them have become part of people's daily necessities because of their decreasing cost, mobility and increasing computational capability. The Internet of Things (IoT) is made up of a wide range of smart gadgets that work together to bring convenience and accessibility to people's lives. The advantages of the Internet of Things are numerous, and its applications are transforming the way we work and live. It also opens up new possibilities for collaboration, growth, and knowledge sharing among other entities. With a sharp increase in the number of IoT devices, these interconnected smart devices can be deployed in a variety of fields and their applications include but are not limited to smart homes, smart cities, environment, agriculture, smart grid, industry, healthcare, and transport. Application domains of the IoT are illustrated in Figure 1.



IoT devices, on the other hand, cannot implement sophisticated security policies due to their low power and limited computational capabilities. As a result of the high number of interconnected IoT devices, adversaries' attacks are rapidly increasing. Because IoT device users and vendors are under-informed on the dangers of IoT security, these devices are becoming a source of potential threats. Attackers can gain control of certain internal and open environments by accessing and probing into IoT devices (e.g., water outages, (e.g. water outages, shortage of public electronic supply and tampering with the functionality of devices). Such security threats are concerning, a house attached to any IoT device is an open invitationto attackers. In light of the above- mentioned security risks for IoT devices, it is vital to have proper access control in order to protect user privacy and prevent on-device data from being leaked. Passwords used to be the only way of user authentication in the IoT, but times have changed. In the past decade, biometric technology has developed in leaps and bounds and has swiftly spread to almost every corner of our daily lives as a more reliable method of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

authentication. With the popularity of smartphones, it is a winning combination of mobile phones and biometrics in the consumer market, allowing biometric authentication to be more widely accepted. this paper presents an in- depth review of current research in biometrics for IoT security, especially focusing on authentication.

1.1 Fingerprint

A fingerprint is a mark left by the friction ridges of an individual's fingerprint. Fingerprints have been used in personal identification applications for centuries due to their convenience and high recognition accuracy. The fingerprint pattern of ridges and valleys located on the fingertip surface is determined in the early stage of fetal development. Different persons fingerprints are different, including if they are identical twins. Fingerprints are highly preferred because of their high recognition accuracy and user Acceptability. Due to physiological, behavioral and environment factors in the biometric acquisition process, biometric uncertainty and noise in biometric authentication systems are inevitable, such as elastic distortion in fingerprint images [54]. It is most likely that samples from the same biometric trait captured at different times or under different conditions are different. Such variabilities may lead to authentication failure in a genuine attempt or fake success in an imposter attempt. A typical biometric authentication system is demonstrated in Figure 3. Biometric authentication is composed of two phases, namely the enrollment phase and the verification phase. In the enrollment phase, a set of features are extracted from the user's biometric image (e.g., fingerprint image and/or face image) and stored in a central database or on a smartcard as template data. In the verification phase, the query's biometric features are extracted in the same way as the enrollment phase and then compared against the template data in the matching module. If the similarity score between the template data and query data is larger than a predefined threshold, the verification is successful; otherwise, it is unsuccessful. Based on the number of biometric traits employed, biometric authentication systems can be categorized into single- and multi- modal biometric authentication systems, which are summarized in Fig. 2

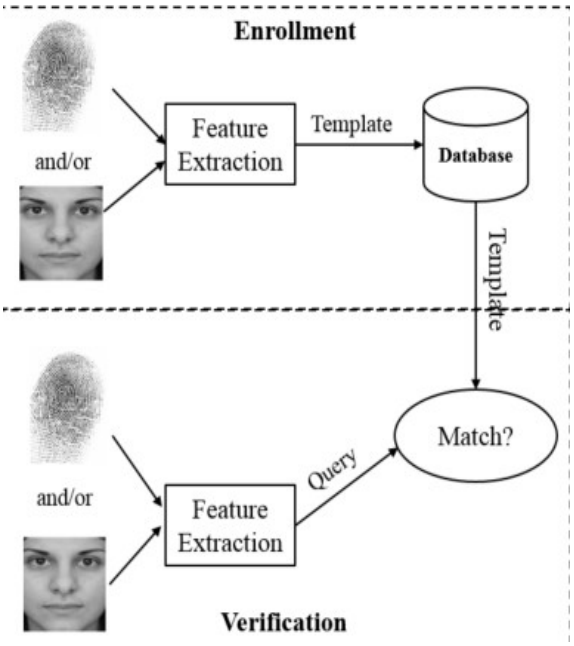


Fig. 2

Single-Modal versus Multi-Modal Biometric Authentication Systems:

Single-Modal Biometric Authentication Systems:

A single-modal biometric authentication system uses information from only one biometric trait (e.g., fingerprint or face) for user authentication to prevent unauthorized access to IoT devices and services. A biometric-based authentication system offers convenience and strong security compared to conventional password- based authentication. Single-modal biometric authentication systems using different traits that appear in existing articles are reviewed below.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

Fingerprint

Devikar et al. proposed an attendance system applying fingerprint based biometric authentication on a portable IoT device. Moreover, the cloud is used to store the attendance records, making data easy to be accessed and retrieved. Shah and Bharadi introduced how to build a low-cost biometric system using Raspberry Pi, which is similar to a credit-sized mini-computer. In this study, the Raspberry Pi is used as a remote node and the enrolled biometric information (e.g., fingerprint data) is encrypted by a cryptographic algorithm and stored in the cloud. In this paper, a fingerprint-based authentication system is implemented with Raspberry Pi together with several types of sensors.

Multi-Modal Biometric Authentication Systems

The term "multi-modal biometrics" refers to the utilisation of various biometric data sources. To increase recognition accuracy, multi-modal biometric systems incorporate biometric information from other biometric traits (such as the face and fingerprints). Better recognition accuracy and more security are two clear advantages of a multi-modal biometric system over its single-modal rival. Multi-modal biometric systems gather and combine data from multiple traits to increase recognition accuracy. Multi-modal biometric systems outperform single-modal biometric systems because the fused data are more discriminative. Multi- modal biometric systems are more reliable in terms of security. Another modal can still attempt to get authentication if the first one fails for an unclear cause. Additionally, the usage of multi-modal biometric systems makes it more difficult for attackers to forge a person's many biometric features.

Macek et al. assumed that it is possible to record iris and facial images concurrently with a multimodal biometric system since more and more IoT devices are outfitted with high- resolution cameras. In this study, fiducial point localization and Gabor filtering are used to extract biometric features from taken photos of the face and iris, which are then saved as templates on IoT devices.

Users of IoT devices are recognised and authenticated at the authentication step using the saved templates. Hassen et al. retrieved a private key using multi-modal biometrics (fingerprint and finger- vein) to verify and validate blockchain transactions in order to increase network security. The outcomes of the experiments show that the suggested approach achieves a high security level in protecting against spoofing and signature forging with high throughput and low latency. However, no combination is infallibly superior to the others, and the choice of combinations depends on the application. The use of multi-modal biometrics has advantages and disadvantages. How to successfully combine and/or fuse numerous biometric traits is still up for debate, and the precise cost of doing so is not known. Single-modal biometric identification systems that use a single biometric feature in real-world applications face problems with felt data noise, intraclass variance, and interclass similarity, which can impair recognition accuracy. By combining numerous sources of data utilising various fusion methodologies, such as feature-level fusion, score-level fusion, and decision-level fusion, multi-modal biometric authentication systems, in contrast, frequently outperform their single-modal equivalents.

Uncertainty of Biometric Data Biometric Data

Contain many uncertainties such as intraclass variability and interclass similarity. Using the most common biometric authentication, fingerprint recognition, as an example, when a contact sensor is used to capture live finger images, nonlinear distortion and rotation of fingerprints are inevitable due to skin elasticity, skin moisture content, finger displacement, contact pressure, sensor noise and imaging methodology. Because of the uncertainty in the captured fingerprint data, matching between query and template fingerprints could fail. Therefore, biometric authentication is inherently a probabilistic task and there is inevitable uncertainty and the risk of error, although the technology and the system itself behave as designed. Despite these difficulties, there is ongoing research to improve the quality and discriminative power of biometric data as well as the matching performance of biometric authentication systems, such that their role in safeguarding IoT security is more effective.

II. LITERATURE REVIEW

Single-modal biometric identification systems, which rely on a single biometric feature, have problems with noise in the sensed data, intraclass variance, and interclass similarity, which can impair recognition accuracy. Contrarily, multi-modal biometric identification systems frequently perform better than their single-modal counterparts by combining numerous sources of data using various fusion methodologies, including feature-level fusion, score- level fusion, and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

decision-level fusion. Due to Multi-Modal Biometric Authentication's ability to produce more precise results, it may be more useful in forensic or criminal justice applications.

III. CONCLUSION

This study examines a variety of biometric methods. Investigates biometric systems For the sake of IoT security, biometric-based technologies are being scrutinised. Contemporary biometric authentication systems are studied and classified as single-modal or multi-modal biometric authentication systems, depending on the types and quantity of biometric attributes utilised. The following future research directions are suggested. Because no single biometric feature can match the requirements of all IoT applications, deciding which biometric qualities are suitable for IoT-oriented biometric authentication is a tough task that requires additional research. Furthermore, while multi-modal biometric systems can reduce biometric uncertainty and give higher authentication accuracy than single- modal biometric systems, the additional cost (e.g., additional processing and computing time) must be addressed. Due to the resource constraints of IoT devices, research into the design of efficient and cost- effective multi-modal biometric systems is critical.

REFERENCES

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

[2]. ABI Research Forecasts 95% of Smartphones to Feature Fingerprint Sensors by 2022. Website-http://www.biometricupdate.com/201705/abi-research-forecasts-95-of-smartphones-to-feature-fingerprint-sensors-by-2022 (accessed on 1 July 2021).

[3]. Devikar, P.; Krishnamoorthy, A.; Bhanage, A.; Chauhan, M.S. IoT based biometric attendance system. Int. J. Adv. Res. Comput. Commun. Eng. 2016.

[4]. Shad, D.; Bharadi, V. IoT based biometrics implementation on Raspberry Pi. Procedia Comput. Sci. 2016.

[5]. 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.