iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4306

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: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Lightweight Biometric System for Internet of Things (IoT) Security

[1]Mrs. S. Subhasini, [2]Dr. V. Kavitha, [3]Mrs. B. Sathyabama, [4]N.Sunil Srinivasan
[1, 3]Assistant Professor, [2] Professor, [4]PG Studnet
[1]Department of computer applications (BCA), Hindusthan College of arts and science,
[2, 3, 4]Department of MCA, Hindusthan College of arts and science

Abstract: ***The "Internet of things" (IoT) is a important topic of discussion both in the place of work and outside of it. Basically, IoT is a idea of between any device to the internet. Many IoT devices are power-driven by batteries of inadequate life and collected of electronic parts of restricted capacity. Therefore, power efficiency is a vital requirement for any IoT tool with limited possessions in conditions of storage space, power, and computing capacity. The proposed system employs a block reason operation based algorithm to decrease the biometric feature volume in a straightforward and well-organized way. Experimental outcome express that with a much reduced feature size, the proposed lightweight biometric arrangement still maintains high accuracy. It is value noting that any substantial reduction in memory and computing cost is of assistance for resource-con-strained IoT strategy.***

Keywords: Internet of Things (IoT), Interoperability, Privacy, Security vulnerability, Internet

I. INTRODUCTION

The Internet of Things (IoT) is an active universal information system consisting of Internet-connected items, such as Radio frequency identifications, sensors.

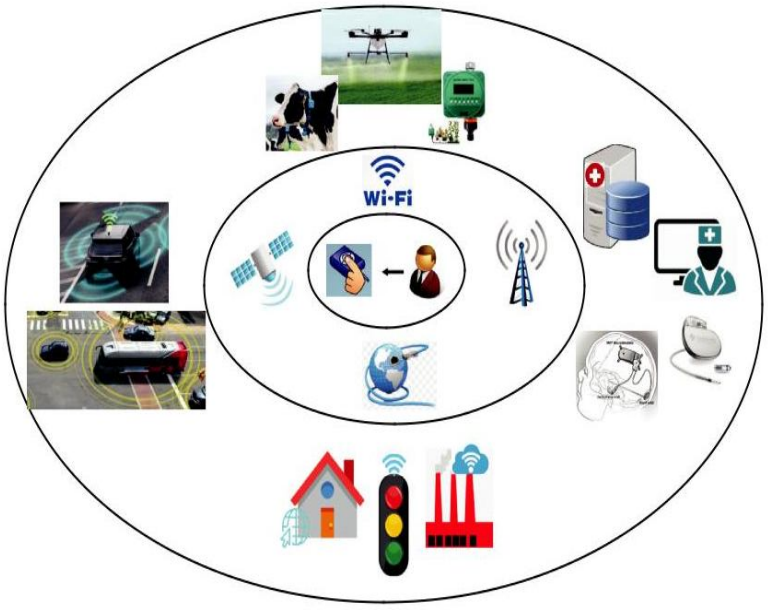


Figure 1. Framework for user authentication in IoT.

Green IoT leads to a lot of benefits, a smaller amount carbon production and pollution, and longer life and lesser volume of resource-limited IoT plans with the constant growth of IoT strategy into daily use for the purpose of simplifying people life Therefore, safety is another huge face up to for IoT development. IoT protection mainly includes aspects of securing composed data, encrypting communication, and user verification. Among them, user authentication is a key in to an IoT security system and plays a critical role in creating a trust between IoT users and devices, and fighting spoofing attacks.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

II. BIOMETRICS IN THE IOT

The Internet of Things (IoT) is competent to fix various entities collectively through the Internet, such as mobile device, cars, and sensors. Biometric-based detection is a rising confirmation technology in the IoT era with bio-metrics becoming a regular feature on more and more IoT devices.

In [1], Habib *et al.* planned a biometric authentication arrangement specifically for IoT in eHealth. The proposed structure is related to the patient's biometric features and radio fingerprinting. In [3], the authors presented a face and iris-based multimodal biometric authentication system on some IoT devices, where a high value camera is built in to attain images of iris and face at the same time. In [4], by joinng a user's hand geometry scan and a series of gestures, the proposed authentication system achieves security defense and access power on IoT devices. In [5], Prakash and Venkatram implemented the fingerprint recognition technique in IoT for a home security system. The implementation was carried out in Raspberry Pi along with a set of hardware. In [6], Karimian *et al.* used the electrocardiogram (ECG) to afford user authentication within an IoT system model. Their findings show that ECG biometrics is extremely secure and dependable as well as easy to implement. In [7], a secure and well-organized biometric-based algorithm was proposed to offer remote authentication services. The proposed algorithm is not computationally costly, and the storage space required by the biometric pattern is sensible.

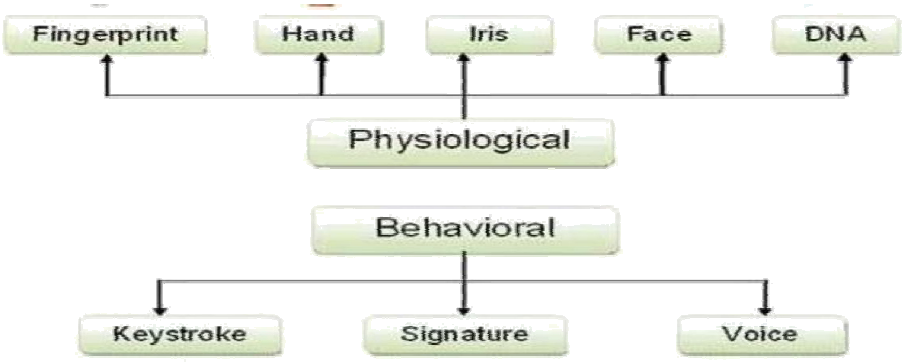


Fig2.Lightweight biometric system

The entire development of the proposed lightweight bio-metric system is illustrated in Fig. 2 and detailed as follows.

1) *LEVEL 1* — minutiae extraction: In the user and biometric module, the user who desires to access an IoT device through the biometric component presents his/her finger to a mobile device ready with a fingerprint sensor. The user's fingerprint representation is acquired by the fingerprint sensor, and a set of *N* finer points are extracted from the finger-print image.
2) *LEVEL 2* — binary feature generation: The extracted minutiae set is input to the MCC algorithm, which associates a local feature descriptorwith each minutia. The local feature descriptor of the MCC encodes the spatial and direction-al relationships between each reference/center minutia and its neighbor minutiae in a prescribed range
3) *LEVEL 3* – block logic operation: The *N* binary strings obtained in Step 2 form feature set *B*. Sup-pose that each binary string has *a* bits. In order to save memory and computing cost in the fin-gerprint matching process that occurs on the IoT device, we propose a block logic operation to be applied to the binary strings in feature set *B*. Specifically, each binary string is divided into small blocks, and each block is of length *b*.
4) *LEVEL 4* — matching: Typical biometric authen-tication involves two stages, the enrollment stage and the verification stage. This is largely applicable to biometric-based authentication in the IoT envi-ronment. The only difference is that in the enroll-ment stage, the template feature set generated by Steps 1–3 is stored in the IoT devices before they are deployed

III. PRESERVATION AND RESEARCH CONTRIBUTIONS

To make biometric-based user authentication better suited for resource-limited IoT devices, in this article we propose a Privacy-preserving light-weight fingerprint authentication system.

1. First, to save the memory and computation-al cost of resource-limited IoT devices, the proposed lightweight fingerprint biometric system performs a block-based XOR operation on the minutia features extracted by the MCC algorithm. In this way, the fea-ture size can be reduced by an adjustable amount depending on different parameter settings. With feature size reduced,

precious resources (e.g., memory space and com-puting cost of IoT devices) are spared. The proposed block logic operation also makes a congruous enhancement to the original MCC algorithm in terms of improving energy efficiency.

2. Second, on the security face, the proposed system can protect biometric feature facts of not only the IoT devices but also the original biometric template itself in an efficient manner. Clearly, this is an advantage over the original MCC algorithm.

IV. THE PROPOSED LIGHTWEIGHT BIOMETRIC SYSTEM

The pro-posed system protects the original biometric model from being compromised by an attacker.

Figure 1. depicts the entire framework of the pro-posed system in an IoT environment. Specifically, the framework used for authentication between the user and various IoT devices consists of three types of parts. They are:

1) The user and biometric module that are included in the inner circle

2) The Internet providers that constitute the middle circle

IoT devices in all types of applications that are situated in the outer circle metrics, minutiae are an essential local characteristic in a fingerprint image, classified by ridge endings. Each minutia can be represented by the x; y coordinates in the Cartesian coordinate system, the minutia's orientation and the minutia type. For the proposed system, minutiae are extracted by using a marketable software package.

A. The Proposed Light-Weight Biometric System Aims To Offer User

An IoT device gives improved security. Since biometric systems offer safe access to IoT devices, the compromise of the biometric structure means the compromise of the IoT device on which the biometric system is implemented. Therefore, the security of the biometric system itself is crucially important.

Methods	Block length	FVC2002 DB2	FVC2002 DB3
Reproduced MCC [8]		0%	1%
Proposed method	3 bits	0%	1%
	5 bits	0%	1%
	30 bits	0%	3%

Table 1. System presentation under different parameter settings in comparison to the original

V. SYSTEM PERFORMANCE EVALUATION

The presentation of the proposed system is evaluated by three indicators, namely false rejection rate (FRR), false acceptance rate (FAR), and equal error rate (EER). Specifically, in the authentic matching tests, the first fingerprint picture is considered as the pattern and compared to the second fingerprint representation of the same finger. The result of real matching tests yields the FRR, as the FRR is definite to be the ratio of unsuccessful authentic matching try to the total genu ine matching attempts

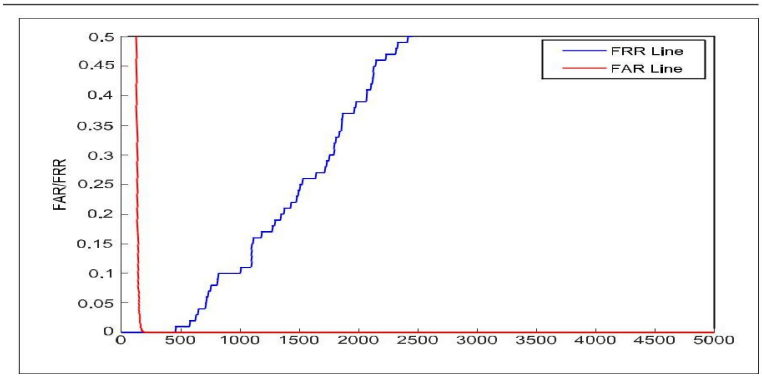


Fig3.Score Threshold

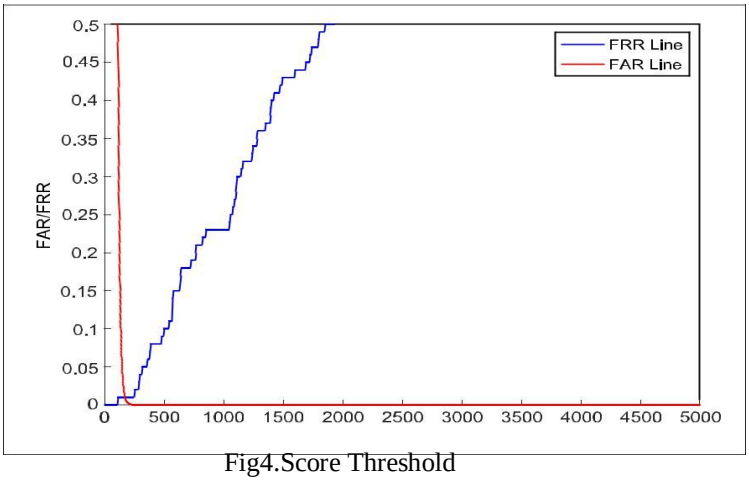


Fig4.Score Threshold

VI. SECURITY BOMETRIC ANALYSIS SYSTEM

The proposed lightweight biometric system focus to offer user authentication to IoT devices with developed security. Since biometric system gives secure access to IoT devices, compromising the biometric system means compromising the IoT device on which the biometric system is implemented. Therefore, the security of the bio-metric system itself is vitally important.

If a biometric template stored on the IoT device is stolen by an attacker, he/she can retrieve all the sensitive information, including the biometric template. With the raw biometric tem-plate acquired from an IoT device, the attacker can reconstruct the original fingerprint feature data. What makes things worse is that other IoT devices may also use the same biometric template from the same user.

It is well known that the unique fingerprint feature data can never be distorted, so the attacker can apply cross-matching on different IoT devices with the restored fingerprint information. Even the safety of the whole IoT network can be at risk if the original biometric pattern is unprotected.

The proposed block logic procedure could not only decrease the biometric feature size, but it also controls the original fingerprint template. Even if the attacker obtains the size-reduced feature vector, the maximum merit of the XOR operation is its low computational intensity and its simplicity in implementation [14]. Moreover, the future block -based XOR is different to the conventional XOR operation, *message key*

VII. PURPOSE

A. Basically considered to ensure safe recognition purposes with extremely optimized usage of accessible technologies and resources.
B. Create no-password criteria in the range of interfaces selling with confidential verification systems.
C. Inculcate decentralization of the biometric systems and offers a greater encryption standards.

VIII. APPLICATIONS

Biometric attendance system, security and encryption procedures are duly incorporated into variety of fields for application on a greater scale. What stands to create the perfect interpretation of these “secure systems” is the highly revolutionized “Internet of Things” technology that facilitates better assurance of operation for greatest security standards.

A. *Banking and E-Payment:* Payment solutions through online or mobile mode, Block chain Systems, E-Trading facilities, and the like.
B. *Business and business enterprise levels:* Facilitate certified Employee Access (direct or remote).
C. *Individual User Level:* IoT features in smart solutions for homes, cars, and other personal belongings, etc.
D. *Physical condition Care Organizations:* Easy recovery and monitoring of the equivalent user data for better investigation of health statistics.

IX. FEATURES

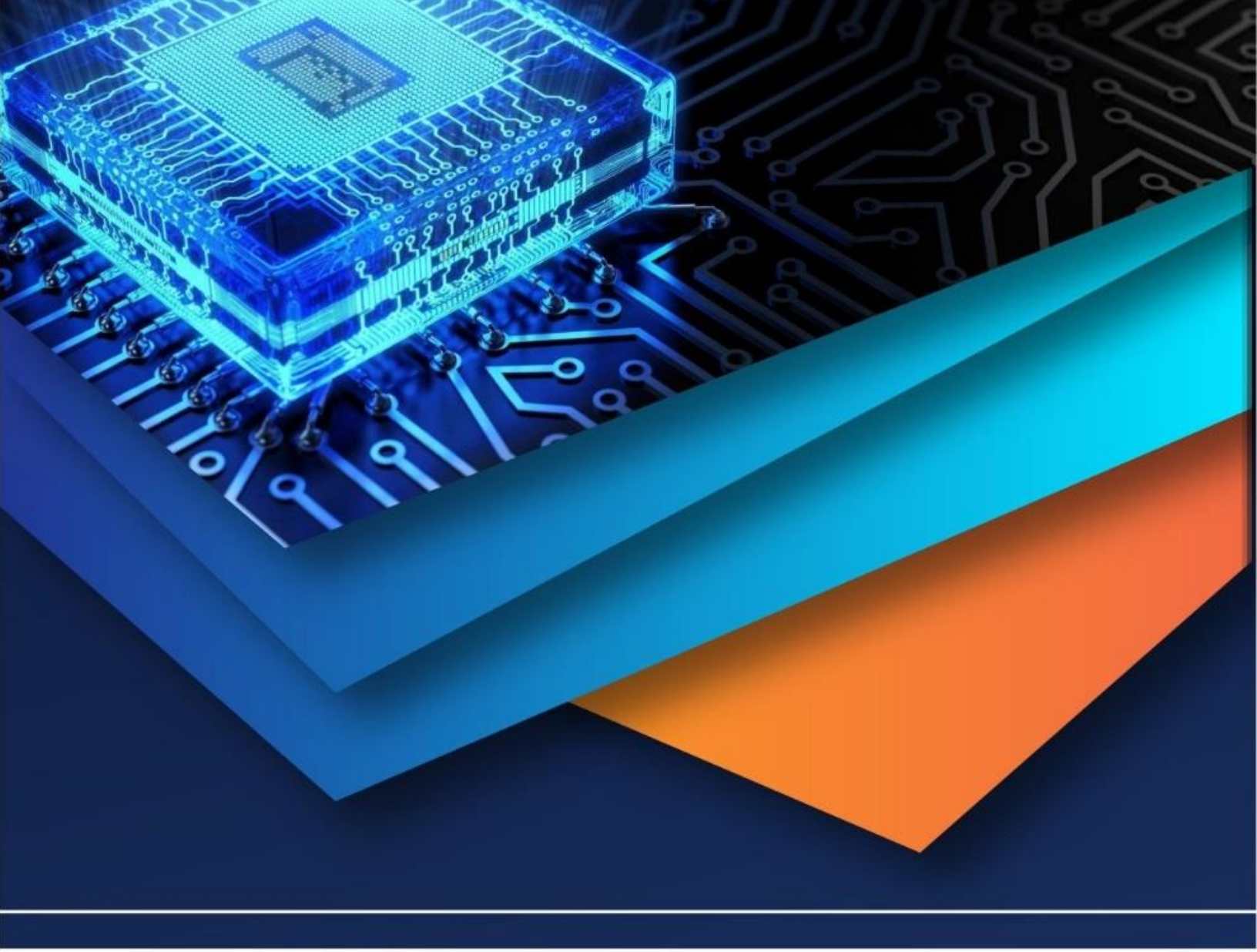
A. Complete authentication with full time security feature.
B. High end monitoring of the secured systems on the go.
C. Full time support systems to transaction with any type of issues generated during the corresponding action.
D. Smart and inventive user boundary to make possible better user experience
E. Personalization features particularly in conditions of the desired equipment.

X. CONCLUSION

Biometrics in IoT will not only unchain bank apps, email accounts but also cars, homes and many other things. "We conventionally guess that biometric sensors, which includes work time management and premise security entry consoles, will entirety at least 600 million "Internet of Things" links by the upcoming years.", there will be uninterrupted applications giving both convenience and security in a variety of industries such as: smart home, automotive industry, finance, healthcare, etc. which will only be not enough by human's thoughts. Energy ability is necessary for any biometric system deployed in the IoT environment. In this article, we have proposed a lightweight biometric system for protected user authentication, which is particularly designed for resource limited IoT devices. Moreover, a block logic procedure based algorithm is developed to decrease the feature size so as to save both memory and computational cost, thus improving the energy efficiency of IoT devices. The experimental results show that the proposed system is beneficial for saving memory space and computing time of IoT devices, which is of practical implication in the IoT scheme of things. As for future work, more efforts will be place into finding stable feature representations and manipulative secure template security algorithms in the mobile environment.

REFERENCES

[1] K. Habib, A. Torjusen, and W. Leister, “A Novel Authentica-tion Framework Based on Biometric and Radio Fingerprint-ing for the IoT in eHealth,” Proc. Int’l. Conf. Smart Systems, Devices and Technologies, 2014, pp. 32–37.
[2] C. Zhu et al., “Green Internet of Things for Smart World,” IEEE Access, vol. 3, 2015, pp. 2151–62.
[3] N. Maček et al., “Multimodal Biometric Authentication in IoT: Single Camera Case Study,” 8th Int’l. Conf. Business Info. Security, Belgrade, Serbia, 2016, pp. 33–38.
[4] L.-P. Shahim et al., “Cost-Effective Biometric Authentica-tion Using Leap Motion and IoT Devices,” 10th Int’l. Conf. Emerging Security Info., Systems and Technologies, Nice, France, 2016, pp. 10–13.
[5] N. S. Prakash and N. Venkatram, “Establishing Efficient Secu-rity Scheme in Home IOT Devices Through Biometric Finger Print Technique,” Indian J. Science and Technology, vol. 9, 2016, p. 8.
[6] N. Karimian, P. A. Wortman, and F. Tehranipoor, “Evolving Authentication Design Considerations for the Internet of Biometric Things (IoBT),” Proc. 11th IEEE/ACM/IFIP Int’l. Conf. Hardware/Software Codesign and System Synthesis, 2016, p. 10.
[7] S. Roy, S. Chatterjee, and G. Mahapatra, “An Efficient Bio-metric Based Remote User Authentication Scheme for Secure Internet of Things Environment,” J. Intelligent & Fuzzy Systems, vol. 34, 2018, pp. 1403–10.
[8] Internet of Things - Applications and Challenges in Technology and Standardization”, Debasis Bandyopadhyay · Jaydip Sen,Wireless Personal Communications manuscript.
[9] “Internet of Things”,Feng Xia, Laurence T.Yang, Lizhe Wang and Alexey Vinel, ,INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS, Volume 25, Issue 9, pages 1101-1102, September 2012 12.
[10] “That ‘Internet of Things’ Thing”, Kevin Ashton, RFID journal, June 2009, http://www.rfidjournal.com/articles/view?4986



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY