

7th International Conference on Communication, Computing and Virtualization 2016

IoT based Biometrics Implementation on Raspberry Pi

Dhvani Shah^a, Vinayak Bharadi^b

^aM.E Scholar, Thakur College of Engineering and College, Mumbai, India, shahdhvani08@gmail.com

^bAssociate Professor, Thakur College of Engineering and Technology, Mumbai, India, vinaya.bharadi@thakureducation.org

Abstract

Developments in the field of Information Technology also make Information Security a devoted part of it. In order to deal with security, Authentication plays an imperative role. In this paper, Biometrics is used for authentication. This paper also describes how biometrics can leverage cloud's boundless computational resources and striking properties of flexibility, scalability, and cost reduction in order to reduce the cost of the biometrics system requirements of different computational resources (i.e. processing power or data storage) and to enhance the performance of biometrics systems' processes (i.e. biometric matching). Here, Raspberry Pi is used to build a low-cost biometric system. Raspberry Pi (RPi) is a credit-sized mini-computer with great capabilities similar to a PC. In this study it is used as a remote enrollment node. The application of Raspberry Pi and cloud computing has given a new direction of research into the field of Internet-of-Things (IoT). Using the biometric technology, a new system of IoT based biometrics is proposed. To maintain the security of biometric traits over the Internet channel from RPi client to the cloud, cryptographic algorithms are applied like RSA and enhanced AES-256. The encrypted biometric information is stored on the cloud and the authentication can be done by Biometric service hosted on Azure cloud. Thus, this papers covers the following topics: attracting power of biometrics into the authentication services, biometrics leveraging the power of cloud, Raspberry Pi- a low-cost IoT device, enhanced AES-256 with Round structure and dynamic S-box generation and the new emerging trend of Internet-of-Things.

© 2016 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Internet-of-Things (IoT); Raspberry Pi (RPi); cloud; biometrics; biometric security; cryptography; AES-256 encryption

1. Introduction

A reliable identity management system is urgently needed in order to conflict the rampant growth in identity theft and to meet the increased security requirements in a variety of applications like forensics, government,

* Corresponding author.

E-mail address: shahdhvani08@gmail.com

transportation, health-care, finances, security, public justice and safety, and education [1] [2]. Information security is concerned with the guarantee of confidentiality, integrity and availability of information in all forms. There are many tools and techniques that can support the management of information security. But system based on biometric has evolved to support some aspects of information security. Biometric authentication supports the aspect of identification, authentication and non-repudiation in information security. Establishing the identity of a person is a critical task in any identity management system. Surrogate representations of identity such as passwords and ID cards are not sufficient for reliable identity determination because they can be easily misplaced, shared, or stolen. Biometric recognition is the science of establishing the identity of individuals based on their measurable biological (anatomical or physiological) or behavioral characteristics [3]. Examples of biological biometrics modalities include fingerprint, hand geometry, iris, face, and ear. Examples of behavioral biometrics modalities comprise gait, signature, and keystroke dynamics. Biometric traits have a number of desirable properties with respect to their use as an authentication token, namely, reliability, convenience, universality, and so forth. These characteristics have led to the widespread deployment of biometric authentication systems [1]. Biometric authentication has to have a high level of accuracy (i.e. Genuine Accept Rate (GAR) and False Accept Rate (FAR)) to be secure and practical for widespread adoption in different applications [4]. The major obstacles to the adoption of biometrics are the lack of accessibility and scalability of existing biometric technology and also the high cost of implementing biometric systems [5].

The biometric databases [6] of the Federal Bureau of Investigation, the US State Department, Department of Defense, or the Department of Homeland Security are expected to develop significantly over the next few years to accommodate several hundred millions (or even billions) of identities. Such expectations make it necessary to formulate highly scalable biometric technology, capable of operating on enormous amounts of data, which, in turn, induces the need for sufficient storage capacity and significant processing power. The first solution that comes to mind with respect to the defined issues is moving the existing biometric technology to a cloud platform that confirms appropriate scalability of the technology, sufficient amounts of storage, parallel processing capabilities and cost reduction.

Further cost of the biometric can be reduced by the use of a low-cost IoT device, Raspberry Pi [7]. The allure of the Raspberry Pi comes from a combination of the computer's small size and affordable price. Raspberry Pi, a credit-card sized low-cost Linux computer can be used to develop a biometric architecture as it has provision of connecting with cameras, fingerprint scanners etc. via USB ports. It has an Ethernet port for Internet connectivity or can be connected to a Wi-Fi hotspot via USB Wi-Fi adapters. In this paper, Raspberry Pi is used as a low-cost, wireless, remote enrolment node and the biometric authentication can be hosted on the cloud as a Software-as-a-Service.

The blend of Raspberry Pi and the cloud has led to the era of an emerging trend. Internet-of-Things (IoT) or machine-to-machine communication (M2M) or machine-to-human communication (M2H). The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and causing in improved proficiency, precision and economic assistance. The advantages of incorporating IoT are low-cost, low space, low power and portability of the entire system of implementation. The Internet of Things will redefine identity management using biometrics to unlock bank apps, email accounts but also cars, homes and personal health databases. IoT will drive device and user relationship requirements in 20 percent of new identity and access management (IAM) implementations by year-end 2016, according to Gartner [8]. Gartner said, "Traditional authentication and authorization for user identities will continue to include devices and services, but will also incorporate expanded machine-to-machine (M2M) communications requirements into expanding digital business moments".

Security of biometric information is another concern to deal with. Since, the biometric traits are leveraging the cloud for storage, performance and scalability features, it is vital to transfer them securely from the client machine to the remote server. Hence, in this paper end-to-end encryption process is proposed. Encryption is done using enhanced AES-256 with Round structure and dynamic S-box generation using pseudo-noise sequence generator. The proposed encryption algorithm will strengthen the security and complexity of the proposed IoT based biometrics system.

Thus this paper aims to build a low cost biometric system which is using a low cost wireless enrollment node and the authentication will be done by Biometric service hosted on the cloud. The captured biometric traits are sent to the Biometric Software-as-a-Service (SaaS) by end-to-end encryption process. Raspberry Pi has verified peripherals for capturing fingerprints and face images: Fingerprint Scanner Futronic FS 88 Optical Fingerprint Reader with Live Finger Detection and the USB webcam. Since the biometric traits are transmitted over an unsecured channel to a remote location, modified AES-256 is applied to have a secure transmission.

2. Related work

One of the main aims of this research is to empower biometrics as an authentication method for security purposes like authenticating for cloud services, unlocking a door, accessing a particular service etc. taking into account the privacy and security challenges that face biometrics when used for remote applications. But the first question to be addressed is: why enable biometrics for authentication?

The security and usability problems [9] of password-based authentication, which is the most commonly used authentication method for secure access, have been reviewed. Many theoretical studies in the literatures show that password-based authentication suffers from a wide-range of attacks including brute force, dictionary, sniffing, shoulder surfing, phishing, and key-logger attacks. In addition, human elements add additional security weaknesses to the password-based authentication. For example, users are likely to write down their passwords, use the same password across-multiple systems, use the same password over a long period of time, and share their passwords with their co-workers, family members, or friends. Sasse et al. [10] experimentally investigate the main causes of password problems such as memorability issues and technical/organizational requirements (e.g., forced change of password). This study concludes that Human Computer Interaction (HCI) techniques can be used to address password problems. Similarly, Yan et al. [11] empirically study passwords memorability and security. In [12] among the biometrics of face, finger, hand, voice, eye, DNA and signature, the face biometric ranks first in the compatibility evaluation of a machine readable travel document (MRTD) system on the basis of six criteria: enrolment, renewal, machine assisted identity verification requirements, redundancy, public perception, and storage requirements and performance.

In [13] authors projected an image capturing technique in an embedded system based on Raspberry Pi boards. Most of the recognition systems are centered on a PC, the portability of which is limited by its weight, size and the high power consumption. In [14], implementation of feature extraction of fingerprint and footprint in Raspberry pi has been conversed. Numerous image processing techniques are implemented on RPi using open source OpenCV library into a Linux platform.

A cloud-based biometric architecture is proposed [15] on Raspberry Pi which has aid in developing a low-cost, scalable and portable biometric system. Peter Peer and Jernej Bule [5] have proposed a face recognition system on cloud, This paper tries to elaborate on the issues such as the most common challenges and obstacles encountered, when moving the technology to a cloud platform, standards and recommendations pertaining to both cloud-based services as well as biometrics, and existing solutions. In [16] authors Dr. Vinayak Bharadi and Mr. Godson D'silva has proposed an architecture for implementing online signature recognition system on a public cloud like Windows Azure. The literature reveals some works that leverage cloud data storage for storing biometric data. Griaule Biometrics [17] introduces a biometric information management system in the cloud, which leverages cloud storage to store biometric data on the cloud. Griaule's biometric information management system protects biometric data using AES encryption while stored and Secure Socket Layer while in transfer.

Raspberry Pi's performances [18] are compared with some current IoT platforms on a general level by computing power, size and overall costs of the solutions. Based on performed scrutiny, it can be stated that Udoo has the best performances among considered IoT hardware platforms, but at the same time its price is quite high. On the other side the detail analyses of Raspberry Pi have shown that as ultra-cheap-yet-serviceable computer board, with support for a great number of input and output peripherals, and network communication is the perfect platform for interfacing with many different devices and using in wide range of applications. Connecting it with WiFi and providing access to the Internet it is probable to set it up for a remote communication, what the Raspberry Pi makes

very suitable for applications in IoT concept. Thus, the benefit of Raspberry Pi lies in its flexibility and unending possibility of its usage aiding the end-users to program it according to their needs and budgets.

3. System Hardware Requirements

The proposed system is a multimodal biometric system, face and fingerprint are the biometric traits under consideration. The hardware requirements for the remote enrolment node are listed below:

In this research, Raspberry Pi 2 Model B is used which costs US \$35. It has 4 USB ports, a HDMI port for connection with the display, micro SD card slot for booting and data storage as RPi doesn't have on-board storage. Also it has 10/100 Mbit/s Ethernet port for internet connection. To make RPi portable in this paper wireless USB Wi-Fi adapter is used. The OS used is Raspbian (Debian wheezy). RPi needs power supply of 5V-800mA (4.0 W) [7]. In order to make the proposed portable, RPi is supplied power through power bank. RPi 2 has 1GB RAM and CPU speed is 900 MHz quad core ARM Cortex-A7. It is a Broadcom2835 System-on-chip hardware. One powerful features of the Raspberry Pi is the row of GPIO pins along the edge of the board as shown in Figure 1. These pins are a physical interface between the Pi and the outside world.

Other peripheral include Passive Infrared motion sensor for the sensing the motion, Futronics FS88 fingerprint scanner and the HP-3100 USB webcam [22] for capturing the biometric traits, finger and face respectively.

4. Proposed System

The proposed IoT based biometrics architecture consists of 3 modules as shown in Figure 2: Raspberry Pi as a remote enrolment node, enhanced AES-256 for security and the Azure cloud for storage, scalability and performance concerns.

The FS88 scanner is interfaced using LibScan API and libusb libraries on the RPi. After the interfacing of webcam the RPi is ready for enrolment process. As soon as the motion sensor detects motion, a desktop application pops up which initiates the enrollment/login process. After the image capturing process, the biometrics are encrypted on the RPi on Mono Developer (C# language) using the proposed AES-256 algorithm along with Round structure and dynamic S-box generation based on pseudo noise sequence generator as explained below. The last step is to upload the encrypted images on the Azure cloud where they are stored in blobs within the register/login containers depending on whether the user is already registered or he is a new user. After the decryption process on the cloud, the original biometric traits are retrieved.

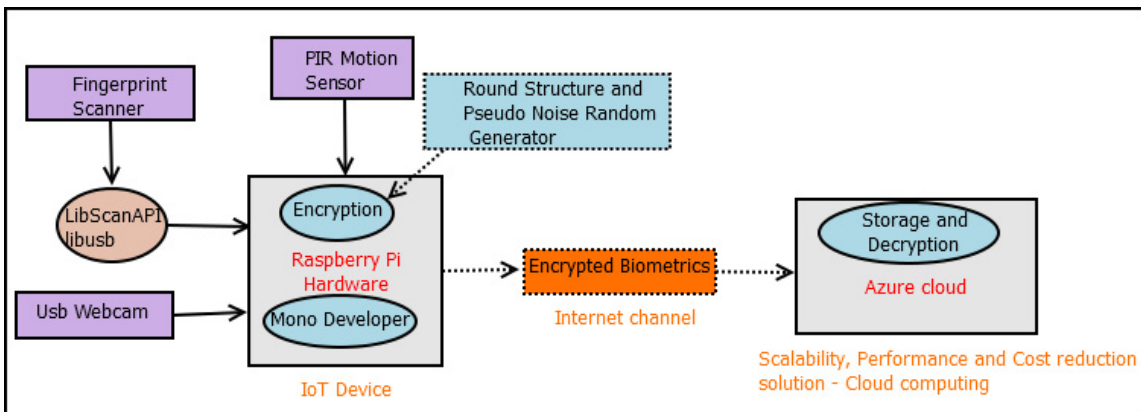


Fig 1: Proposed IoT Based Biometric System.

The proposed AES-256 algorithm is as follows. The biometric images are converted into bits. The key for AES-256 is 512bits which is further broken down into 256-bits each. The 512-bit is randomly generated on the RPi. The KR (first 256-bit) is used for the Round structure and the remaining 256bits are used for the dynamic S-box

generation called as KA. The Round structure goes like this: The input data to the proposed algorithm is 256-bits, again divided into 2 parts LO (first 128-bit) and RO (next 128-bit). RO is XORed with KR, their 128-bit output is XORed LO and then fed into AES-256 algorithm. This forms one round of the Round structure. 14 rounds of Round structure is implemented. Now, the dynamic S-Box generation goes like this: 64bits from KA is fed into PN sequence with 14, 19 and 31 taps. The output is XORed with round key. This output is XORed among itself and used to rotate the standard S-box. The output of the PN sequence generator will be fixed throughout what will differ is the round key for each 14 rounds of the AES-256. Thus 1 round of Round structure includes 14 rounds of AES-256 with different S-box for each round of AES. This adds more complexity and security to the overall system. [19] [20] [21].

5. Results

This section focuses on the results after the implementation of the IoT based system. Results are produced in following way: Raspberry Pi as a remote enrolment node, proposed AES-256 analysis and the uploading of encrypted images to the register/login containers. Figure 2 shows the image capturing application on Raspbian using Mono Develop.

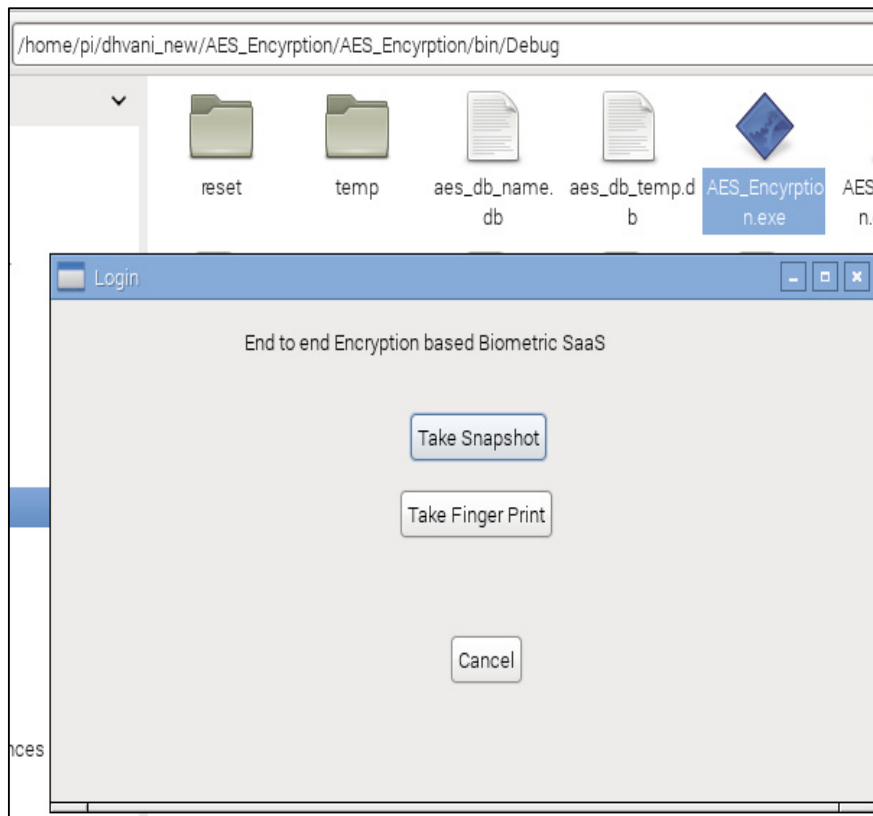


Fig 2: End-to-End Encryption Biometric SaaS application: Home page

Figure 3 and Figure 4 demonstrates the captured biometric data on RPi using the USB fingerprint scanner and the webcam. This highlights the capability of Linux based mini-computer to be a remote enrolment node.

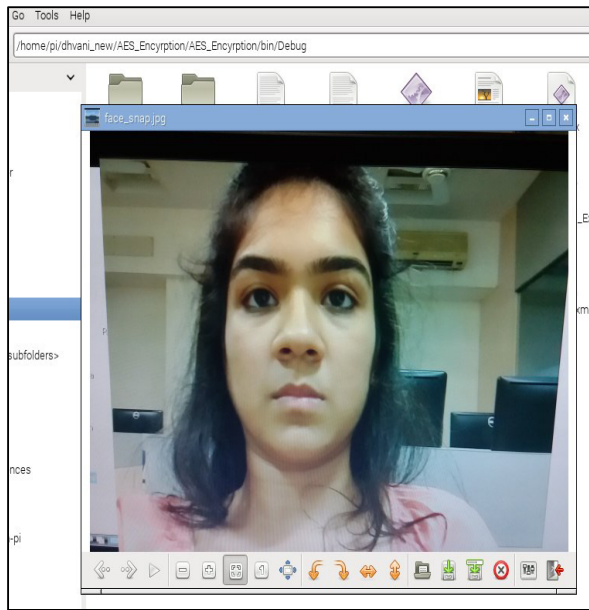


Fig 3: Biometrics Acquisition: Face

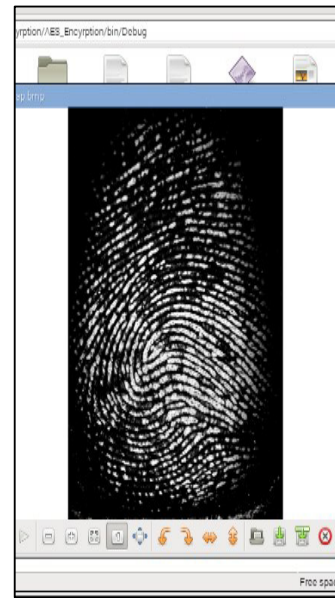


Fig 4: Biometrics Acquisition: Fingerprint.

The next part is to encrypt biometric traits to assure security of the same in-transit to the Azure. The biometric information is converted into cipherdata using the proposed AES-256 algorithm on the RPi client. Table 1 shows the encryption parameters which includes encryption time, CPU and Memory usage of the algorithm on the RPi for both the biometric images. The face captured on RPi is of the resolution 640x480. Since the image is RGB model, the total size in bits is 7372800. Similarly, the resolution of the fingerprint is 320x480 and it is a grayscale image. So, the total size of the fingerprint image is 1228800bits. Hence the total size of biometric traits is 8,601,600 bits which becomes the input to the proposed AES-256 algorithm.

Table 1. Proposed AES-256 parameters

Parameters	
Encryption Time	96980ms
CPU usage	36757504Bytes
Memory usage	21%

Next, on the Linux operating system we have done a comparison of normal AES-256 and the proposed AES-256 with Round structure of 14rounds and dynamic S-box as explained in Section 4. The comparison parameters include encryption time, CPU and memory usage as shown in Table 2. The input to the algorithms is the Fingerprint image whose size is 1228800bits.

Table 2. AES-256 comparison.

Parameters	Normal AES-256	Proposed AES-256
Encryption Time (seconds)	20.45	32.69
Memory usage (MB)	1.23	4.35
CPU usage (%)	19	21
Avalanche effect	0.875	0.90652

The memory required and the encryption time are ofcourse more than the normal AES-256 but as far as security is concerned the proposed AES-256 is more secure. This is evident from the Avalanche effect calculated. Four bits are changed in the plaintext to calculate the Avalanche effect as shown in Table 3 and 4.

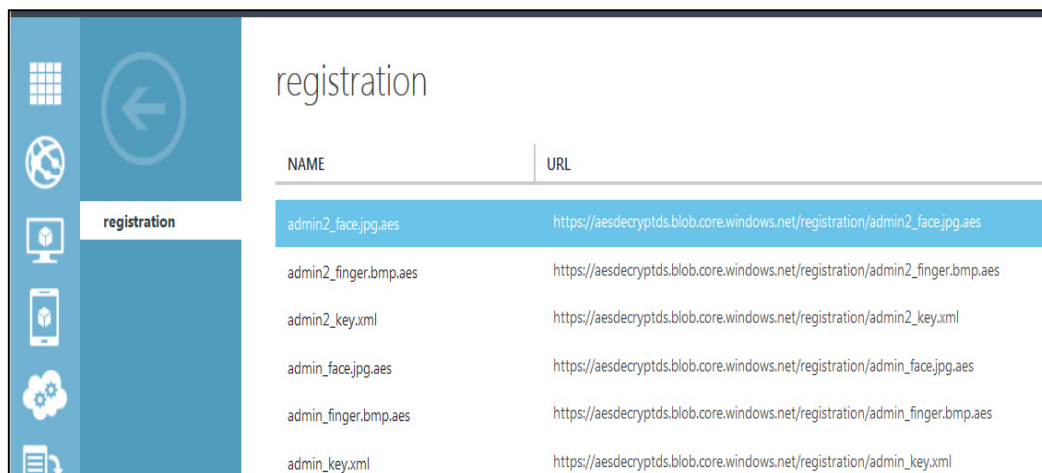
Table 3. Avalanche effect – Normal AES-256

Plain Text	Cipher Text	Avalanche Effect
7D5541C9DE0E3C218E2611219BCCB206	a08dd236c07329980cf28b88c82f0b27	
7D6641C9DE0E3C218E2622219BCCB206	a10e65cab611ee50da0afb879ae45b08	0.875

Table 4. Avalanche effect – Proposed AES-256

Plain Text	Cipher Text	Avalanche Effect
7D5541C9DE0E3C218E2611219BCCB20603087B54B5F10A598E07869C72917142	087085513694d0b2fca18c65ee6ea0b27a5f723ed1fa0503be692de54c88a7c9	
7D6641C9DE0E3C218E2622219BCCB20603087B54B5F10A598E07869C72917142	981d26c9ea22f0dc01c034dc677c014eb97f88cdf8310fc1f6a5949ace54267	0.90652

After the encryption on the RPi, the encrypted images along with key encrypted with RSA is sent to the Azure for further processing. On Azure, we have created Register and Login containers within the blob storage to store the register and login credentials.



NAME	URL
admin2_face.jpg.aes	https://aesdecryptds.blob.core.windows.net/registration/admin2_face.jpg.aes
admin2_finger.bmp.aes	https://aesdecryptds.blob.core.windows.net/registration/admin2_finger.bmp.aes
admin2_key.xml	https://aesdecryptds.blob.core.windows.net/registration/admin2_key.xml
admin_face.jpg.aes	https://aesdecryptds.blob.core.windows.net/registration/admin_face.jpg.aes
admin_finger.bmp.aes	https://aesdecryptds.blob.core.windows.net/registration/admin_finger.bmp.aes
admin_key.xml	https://aesdecryptds.blob.core.windows.net/registration/admin_key.xml

Fig 5: Registration credentials on Azure

For each user, 3 pieces of information is stored in blob storage: cryptographic key, the encrypted images of face and fingerprint. These are successfully uploaded to the Azure cloud. In Fig. 5, the Registration container holds the information about the user entered during the registration process. Similarly during the login process, the login container stores the details of the user.

During the login process, the biometric images are captured and encrypted on RPi and then sent to the blob storage. Now, on Azure a WCF webrole service is deployed which runs the decryption process. The decryption code is written on Mono Develop in C# and is wrapped up into a package and configuration file which is then uploaded on Azure. Thus, RPi consumes the WCF service of Azure PaaS. The decryption parameters like decryption time on

Azure with a VM of 1.75GB RAM and 20GB storage, CPU and memory usage of Azure platform is calculated and given back to the RPi as shown in Table 5. The total size of biometric traits is 8,601,600 bits which becomes the input to the proposed AES-256 algorithm.

Table 5. Proposed AES-256 parameters

Parameters	
Decryption Time	5731.04ms
CPU usage	55455744Bytes
Memory usage	40%

Next, on Azure we have done a comparison of normal AES-256 and the proposed AES-256 with Round structure of 14rounds and dynamic S-box as shown in Table 6.

Table 6. AES-256 comparison.

Parameters	Normal AES-256	Proposed AES-256
Decryption Time (seconds)	1.66	2.33
Memory usage (MB)	22.67	30.45
CPU usage (%)	37	42

The comparison parameters like decryption time on Azure with a VM of 1.75GB RAM and 20GB storage, CPU and memory usage of Azure platform is calculated and given back to the RPi. The input to the algorithms is the Fingerprint image whose size is 1228800bits.

6. Conclusions and Future Work

In this research, we presented a low-cost IoT based biometrics architecture. Raspberry Pi was successfully implemented as a remote wireless enrolment node. Also the encryption module was efficiently executed on RPi. The encrypted biometric traits was sent from RPi client to the Azure cloud for decryption. The proposed system can be used for security and access control mechanisms like unlocking a door, logging details of a person entering and exiting a building, attendance management, accessing a particular service etc. This system can be applied at all places where authentication is required. Avalanche effect depicted that the IoT based biometric system is highly secured.

The future work includes decryption on cloud, incorporation of recognition module on the Azure cloud and hence authentication will be carried on cloud which will increase the performance and scalability of the biometric system. Enhanced AES-256 algorithm is used to handle the privacy and security of the biometric data. Since decryption process is executed on the cloud, the original biometric information of users are within the boundaries of cloud service providers. To solve this issue homomorphic encryption can be used. Unlike traditional encryption, homomorphic encryption allows data processing on the encrypted data. This will assure that users' privacy is not compromised. Biocryptographic systems can be used where biometrics and cryptography are employed together to provide privacy enhanced biometric authentication capabilities.

References

1. Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, Review Article: Biometric Template Security, Journal on Advances in Signal Processing Volume 2008, Article ID 579416.
2. Debnath Bhattacharyya, Rahul Ranjan I, Farkhod Alisherov A., and Minkyu Choi, Biometric Authentication: A Review, International Journal of u- and e- Service, Science and Technology, Vol. 2, No. 3, September, 2009.
3. <http://biometrics.gov/Documents/Glossary.pdf>, National Science and Technology Council's (NSTC) Subcommittee on Biometrics, Biometrics Glossary, 2006.

4. Abdullah A. Albahdal and Terrance E. Boulton, Problems and Promises of Using the Cloud and Biometrics ResearchGate publications, 17th November 2015.
5. Peter Peer and Jernej Bule, Jerneja Zganec Gros and Vitomir Struc., Building Cloud-based Biometric Services, *Informatica* 37 (2013) 115–122 115.
6. E. Kohlwey, A. Sussman, J. Trost, and A. Maurer, Leveraging the Cloud for Big Data Biometrics: Meeting the performance requirements of the Next Generation Biometric Systems, in *Proceedings of the IEEE World Congress on Services*, pp. 597–601, 2011.
7. <http://www.raspberrypi.org>, About raspberry Pi.
8. <http://www.gartner.com/newsroom/id/2944719>
9. Abdullah Abdulaziz Albaldah, Towards Secure, Trusted, and Privacy-Enhanced Cloud, Ph.D. thesis.
10. M. A. Sasse, S. Brostoff, and D. Weirich, Transforming the weakest links human/computer interaction approach to usable and effective security, *BT technology, Journal*, vol.19, no.3, pp.122–131, 2001.
11. Biometrics in the J. J. Yan, A. F. Blackwell, R. J. Anderson, and A. Grant, Password memorability and security: Empirical results, *IEEE Security & privacy*, vol. 2, no. 5, pp. 25–31, 2004.
12. R. Dhannawat, T. Sarode and H.B. Kekre, Kekre's Hybrid Wavelet Transform Technique with DCT, Walsh, Hartley And Kekre Transforms for Image Fusion, *IJCET*, Vol. 4, Issue 1, pp. 195–202, January-February 2013.
13. G.Senthilkumar, K.Gopalakrishnan, V.Sathish Kumar, Embedded Image Capturing System Using Raspberry Pi System, *International Journal of Emerging Trends & Technology in Computer Science*, vol. 3, issue 2, April 2014.
14. S. Sivaranjani and Dr. S. Sumathi, Implementation of Fingerprint and Newborn Footprint Feature Extraction on Raspberry Pi, *IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15*.
15. Shah, D.K.; Bharadi, V.A.; Kaul, V.J.; Amrutia, S., End-to-End Encryption Based Biometric SaaS: Using Raspberry Pi as a Remote Authentication Node, *IEEE sponsored 1st International Conference on Computing, Communication, Control, and Automation (ICCUBEA)*, February 2015, pg. 52 – 59.
16. V. A. Bharadi and G. M. DSilva, Online Signature Recognition Using Software as a Service (SaaS) Model on Public Cloud, *International Conference on Computing, Communication, Control and Automation*, 2015, pp. 65–72.
17. <http://www.griaulebiometrics.com/en-us/biometric-framework>, Griaule Biometric Framework-Griaule Biometrics.
18. <http://www.researchgate.net/publication/272175660>, Mirjana Maksimovic, Vladimir Vujovic, Nikola Davidovic, Vladimir Milosevic and Branko Perisic, Raspberry Pi as Internet of Things hardware: Performances and Constraints.
19. Krishnamurthy G N, V. Ramaswamy, Making AES Stronger: AES with Key Dependent S-Box, *International Journal of Computer Science and Network Security (IICSNS)*, VOL.8, No.9, September 2008
20. Kaul, V.; Bharadi, V.A.; Choudhari, P.; Shah, D.; Narayankhedkar, S.K., "Security Enhancement for Data Transmission in 3G/4G Networks", *IEEE sponsored 1st International Conference on Computing, Communication, Control, and Automation (ICCUBEA)*, February 2015, pg. 95 – 102.
21. Afaq Ahmad*, Sayyid Samir Al-Busaidi and Mufeed Juma Al-Musharafi, On Properties of PN Sequences Generated by LFSR – a Generalized Study and Simulation Modeling, *Indian Journal of Science and Technology*.
22. <http://elinux.org/RPiVerifiedPeripherals>, RPi Verified Peripherals.