Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/76

Biometrics Application on Raspberry Pi for The Internet of Things

Dibyahash Bordoloi[1], Surendra Shukla[2]

[1]Head of the Department Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002
[2]Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002

ABSTRACT

As the field of information and communications technology (ICT) has developed, information security has emerged as an essential subfield to ensure users' privacy and security. In addition, this paper details how biometrics can leverage the cloud's boundless computation power and striking properties of versatility, extensibility, and cost reduction to lessen the burden on budgets caused by the high prices of the biometrics system's needs for various computational resources (like processing power or storage systems) and boost the efficiency of biometrics system operations (i.e. biometric matching). To make a low-cost biometric system, this project uses a Raspberry Pi. The Raspberry Pi (RPi) is a little computer about the width of a credit card that can handle many of the same functions as a full-sized PC. As a remote registration centre, it plays an important role in this study. Microcontroller and cloud computing have opened up a new research frontier in the Internet of Things (IoT) sector (IoT). A novel authentication tokens Web of Things technology is offered to enhance security. When sending biometric features first from RPi client to the cloud, they are encrypted using cryptographic techniques like RSA and enhanced AES-256. When it comes to authentication, nothing beats the convenience and security of a cloud-based biometric solution hosted in Microsoft's Azure cloud. This paper therefore delves into the following topics: Upgraded AES-256 in A round architecture and variable S-box generation, cloud-based biometrics, Raspberry Pi as an inexpensive Iot system, and the emerging Internet of Things are all examples of recent developments. Integrity checks are very important. For the purposes of this work, we resort to biometric techniques for authentication.

Keywords:

INTRODUCTION

A reliable identity management system could help battle the growing problem of identity theft and help industries like forensics, government, transportation, healthcare, banking, security, public justice and safety, and academia meet rising standards for security. The core of information security is the assurance of confidentiality, integrity, and availability of information in any medium. There is a plethora of tools at your disposal to help with information security management. In spite of this, biometrically-based systems have progressed to the point where they can support particular features of data security. Using biometrics for authentication aids in all three areas of IT safety . User

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/76

identity verification is a crucial component of any identity management system. Surrogate representation of identity, such as passwords and identification cards, are not sufficient for safe identity verification since they can be stolen or misused. The field of study known as "biometrics" focuses on the ability to recognise an individual based on his or her distinct biological, behavioural, or phenotypical characteristics. Handprints, biometric traits, irises, cheeks, and ears are just a few examples of how biometrics systems can distinguish between individuals. Modalities in big data . big include things like gait, signatures, and the movements of keystrokes. Biometric features have widespread potential as a s system due to their reliability, mobility, and adaptability. Because of its many advantages, biometric authentication is quickly gaining in popularity. Biometric identity systems need to have both a strong Genuine Acceptance Rate (GAR) and a low False Admission Rate (FAR) to be widely accepted and implemented. One of the main obstacles to biometrics' mainstream adoption is the expensive cost of deploying systems and the complexity of applying biometrics at scale.

The FBI, the US State Department, the Department of Defense, and the Department of Homeland Security will need to collect and store biometric data on 100s, if not billion, of people in the coming years. A huge quantity of storage space and potent computer resources are required to create highly scalable biometrics that can process massive volumes of data in order to achieve these criteria. One obvious solution to these issues is to move current biometric system to a cloud platform that has been proven to have sufficient scalability, memory, parallel process technology, and cost reduction. The low-cost Internet of Everything device Raspberry Pi can be utilised to further decrease the expense of the biometric. The small size and low cost of the Raspberry Pi have helped it gain broad popularity. The Raspberry Pi, a credit card-sized, low-cost Linux computer, can be used to plan a biometric architecture thanks to its USB ports, which can be connected to cameras, fingerprint scanners, and so forth. It supports both wired Ethernet and wireless Internet access via a USB wireless adapter. This research proposes utilising Raspberry Pi as a low-cost, wirelessly, remote enrolment node for biometric authentication residing in the cloud as a Software-as-a-Service.

Concerns about data security arise when using biometrics. To make the most of the cloud's storage, speed, and scalability benefits with biometric characteristics, it is essential that they be transmitted securely from the client machine to the distant server. So, the authors of this paper offer a method of encryption that works from start to finish. The encryption process uses a modernised version of AES-256, specifically the Round structure with dynamic S-box formation using a pseudo-noise sequence generator. With the proposed encryption technology, the proposed IoT-based biometric system will be significantly more complicated and secure**.**

LITERATURE REVIEW

Even though password-based authentication is the most common method currently in use, it has been proved to have safety and usability flaws that make it unsuitable for many applications. Numerous theoretical studies in the literatures show that password-based authentication is vulnerable to a wide range of assaults. Attempts at compromise can captured with key-loggers. Due to human error and other variables, password-based authentication isn't bulletproof. Passwords are most often exposed because their users either keep them written down, use the same password for multiple accounts or websites, or use the same password for a lengthy period of time . Using a

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/76

controlled experimental design, ***Sasse et al.*** investigate the underlying causes of password problems . Results from this study suggest that HCI methods can be used to address password problems. Similarly, ***Yan et al. (2017)*** perform an empirical study on the effectiveness and ease of remembering passwords. Out of six biometrics tested, ***Dhannawat et al***. found that facial recognition worked best with an MRTD system. Factors including enrollment, renewal, the necessity of machine-assisted identity verification, the availability of backup systems, public opinion, storage capabilities, and performance, all play a role.

Senthilkumar et al. suggested a method for capturing images in an integrated system with Raspberry Pi chips. Despite being the industry standard, PC-based identification systems are typically not very mobile due to reasons like their large sleek design and high energy consumption. Sivaranjani et al. discuss how to implement fingerprints and footprint extraction and classification on Raspberry pi. The Raspberry Pi can do a wide range of tasks involving image processing thanks to the OpenCV library, which can be downloaded for free from GitHub and is included in Linux.

Using the cloud-based biometric architecture provided by ***Shah et al.*** on Raspberry Pi, a low-cost, flexible, and moveable biometric system can be created. The goal of this article is to offer a the most in analysis of the challenges, including the most common obstacles and barriers encountered when migrating the new tech to a cloud service, as well as relevant standards and recommendations for fog services and biometric - based, and existing solutions. The ***Bharadi et al.*** proposal provides an architecture for launching a web-based signature recognition service in a public cloud environment, such as Windows Azure. After examining the existing literature, we may assume that several initiatives have used cloud-based storage to protect people's biometric information.

PROPOSED METHODOLOGY

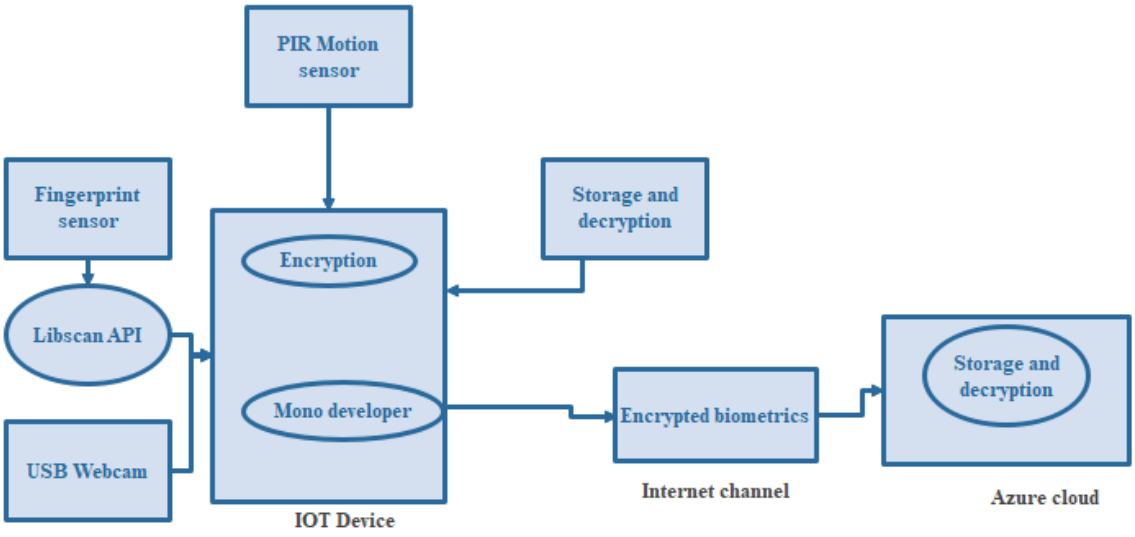

Fig 1: Proposed Architecture

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/76

Figure 1 depicts the three main components of the proposed IoT-based biometrics architecture. Storage, stability, and performance challenges were handled in the cloud by way of Microsoft Azure, while a Raspberry Pi served as a remote registration node.

The FS88 scanner is connected to the RPi over USB using the LibScan application programming interface and the libusb libraries. Once the webcam is set up, the RPi can be registered in courses. When the motion sensor senses motion, it triggers a desktop application that begins the registration and login process. Having captured an image, a Raspberry Pi running Mono Developer (C#) encodes the biometric information to use the recommended AES-256 method, Round architecture, and variable S-box generation based on a simulated noise sequence, as will be displayed in the next sections. After that, you'll upload your encrypted photo to Azure cloud and it will be placed in either the register or login container depending if or not you've already registered. After being encrypted in the cloud, the biometric traits can be recovered in their raw form.

The AES-256 algorithm is a candidate for the next-generation encryption standard. A digital representation of the biometric images is made. The 512-bit key length of AES-256 is split into two 256-bit keys. The 512-bit random number comes from a Raspberry Pi. The Round structure (denoted by KR) is built with the first 256 bits, and the other 256 bits (denoted by KA) are utilised to build dynamic S-boxes. This is how a Round is typically structured: As input, the proposed method receives 256 bits of information, which are then divided into low-order 128 bits (LO) and elevated 256 bits (RO) (next 128-bit). The AES-256 algorithm receives the 128-bit result of XORing RO and KR, which has previously been XORed with LO. There's one complete round of the Round structure here. To date, 14 rounds have been played. This is the current method for creating a dynamic S-Box: The PN sequence, with its 14, 19, and 31 taps, receives the KA's 64 bits. The output of a round-key XOR operation. A typical S-box is inverted by XORing this result with itself. The input to the PN sequence generator remains the same across all 14 rounds of AES-256; only the round keys change. For this reason, 1 round of Round architecture employs 14 rounds of AES-256, each of which has its own special S-box. Because of this, the system will be more complicated and secure.

RESULTS AND DISCUSSION

Here, we'll analyse the performance of the Internet of Things-based system after it was placed into use. This is the process by which the results are produced: A Raspberry Pi is proposed as a distant enrollment node, and AES-256 analysis and encrypted picture uploads to the registration containers are suggested as means of securing the data. The second stage, encryption of biometric features, ensures the security of the data during transmission to Azure. The biometric data is encrypted using the recommended AES-256 technique on the RPi client. Parameters of the algorithm's encryption are displayed in Table 1; this includes the time it took to decrypt the photographs, the number of CPU and Memory consumed, and the storage capacity space required by the method. The 640x480 pixel resolution of the RPi face is standard**.**

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/76

Parameters	Values
CPU usage	36757504
Memory usage	21
Encryption time	96980

Table 1: Implemented AES-256

There are a total of 7372800 bits because it is an Image file. There is a 320x480 grayscale fingerprint image available. In total, the recognition system is 1228800 bits in size. The total number of biometric characteristics is 8,601,600 bits, and this is the number that must be fed into the proposed AES-256 technique.

Then, we examined the differences between the two versions of AES-256 running on Linux, the default implementation of AES-256 and the proposed variant, AES-256 with The round organization of 14rounds and flexible S-box. The outcomes of an evaluation of many features of encryption, including time required and resource requirements, are shown in Table 2. The 1228800-bit Fingerprint image is used as the input for the algorithms.

Parameters	General AES-256	Proposed AES-256
Avalanche effect	0.95	0.99
Memory usage	1.65	5.89
CPU usage	18.0	22.0
Encryption time	21.35	35.6

Table 2: Analysis of AES-256 versus other ciphers.

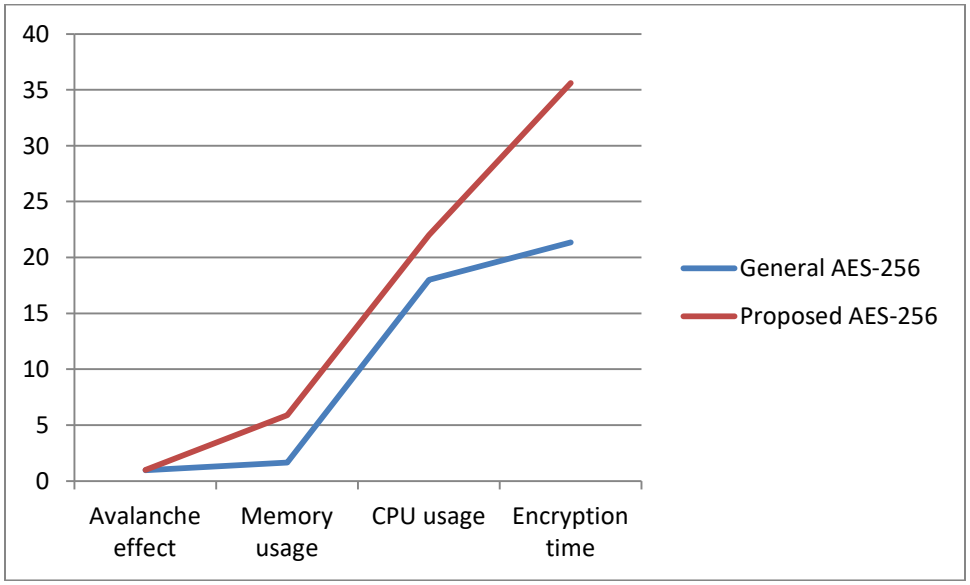

Fig 2:Comparing implemented and general AES-256

According to the conventional AES-256, the suggested AES-256 will require more memory and

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/76

more time to encrypt data, but it will also provide a higher level of security. This is shown by the calculated Avalanche effect. Modifying four plaintext bits yields the result needed to calculate the Avalanche effect. Following encryption on the RPi, the images and a key encrypted with RSA are uploaded to Microsoft Azure. We have segregated the registered and login data into their own container in Azure's blob storing for maximum security.

All biometric information, including cypher keys, encrypted photos of the user's face and fingerprints, and other sensitive information, is stored in a blob database. Migrating to Microsoft's Azure cloud went smoothly. The Registration object stores the user information entered during registration. At each stage of the login process, the login container serves the same function.

Images of the user's biometrics are captured by the RPi and during user login, encrypted locally, and then uploaded to blob storage. Current decryption is being handled via a WCF webrole service deployed in Azure. Using Mono Develop, we write the C#-based decryption code, package it up with the necessary configuration file, and upload it to Azure. Therefore, Azure PaaS WCF service is utilised by the RPi Table 5 shows the returned decryption parameters to the RPi, such as the CPU and memory usage of the Azure platform, the decrypt duration on Azure with a VM of 5.54 GB RAM and 20Gb of internal storage, and so on. The suggested AES-256 algorithm takes as input a set of biometric characteristics that together amount to 8,601,600 bits in length.

Parameters	**Values**
CPU usage	36757504
Memory usage	21
Decryption time	96980

Table 3: Implemented AES-256 for decryption

Parameters	**General AES-256**	**Proposed AES-256**
Memory usage	2.65	7.89
CPU usage	18.0	22.0
Decryption time	21.35	35.6

Table 4: Analysis of AES-256 versus other ciphers for decryption

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/76

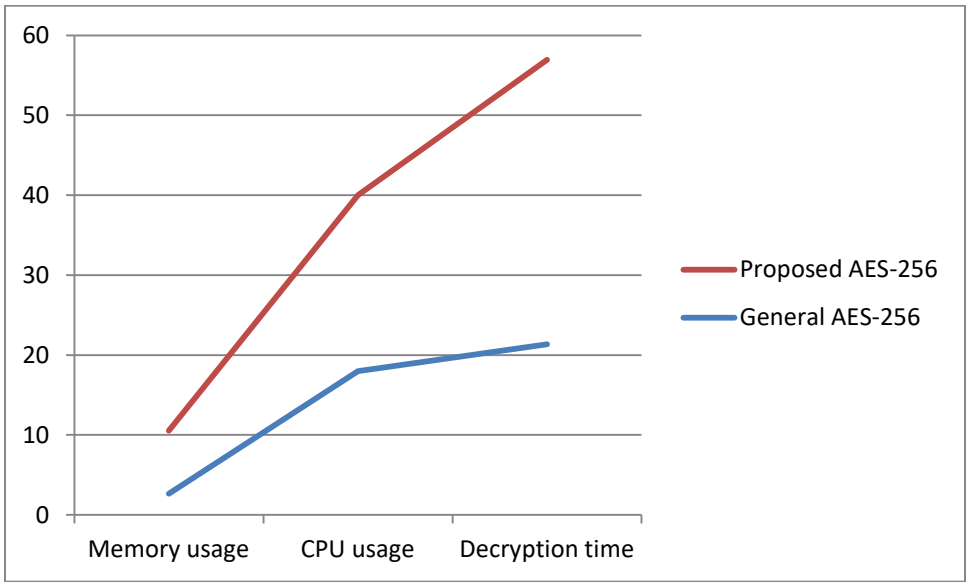

Fig 2:Comparing implemented and general AES-256 during decryption

CONCLUSION

As part of our research, we presented a low-cost biometrics infrastructure that makes use of the Internet of Things. The use of Raspberry Pi as a wireless enrollment node in faraway locations proved to be successful. The encryption component also worked flawlessly on RPi. The RPi client's encrypted biometric features were sent to Microsoft's Azure cloud for decoding. The proposed system can be used to unlock doors, keep track of who enters and exits a building, record attendance, allow the use of a restricted system, etc. There will be no restrictions on where this system can be used because of the authentication procedure. The avalanche effect proved how secure the IoT biometric solution actually was.

Decryption in the cloud and the addition of a recognition module hosted on Microsoft's Azure cloud are two steps toward making biometric authentication a cloud-based procedure that will boost both the system's performance and its scalability in the near future. Biometric data is encrypted with a more secure AES-256 technique, ensuring its privacy and security. Since decryption occurs in the cloud, customers' original biometric data is also under the authority of their cloud services. Homomorphic encryption provides a practical solution to this issue. While traditional encryption methods prevent any manipulation of encrypted data, homomorphic encryption allows for this. The privacy of our users is ensured with this system in place. When biometrics and encryption are used together, the result is biometric authentication with increased privacy.

REFERENCES

1. 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.
2. G.Senthilkumar, K.Gopalakrishnan, V.Sathish Kumar, Embedded Image Capturing System Using Raspberry Pi System, International Journal of Emerging Trends & Technology in

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/76

Computer Science, vol. 3, issue 2, April 2014.

3. 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.
4. 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, Contro,l and Automation (ICCUBEA), February 2015, pg. 52 – 59.
5. 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.
6. 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.
7. 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