Online available at www.iahrw.com
International Journal of Science, Engineering & Computer Technology
ISSN: 2231-508X, UGC Approved Journal (Sr. No. 4812)

Biometric Fingerprint Identification Based on IoT

Anand
Assistant Professor, Keshav Mahavidyalaya, University of Delhi, Delhi

A B S T R A C T

This paper discusses a proposed system offering a decentralized biometric solution for identification based on IoT. The proposed solution offers portability, energy efficient design, a distributed secure finger template storage mechanism and an encrypted channel for wireless network communication. The key feature is that the biometric data is preserved and the operations are performed on a unique ID. The biometric system based authentication offer several advantages over the traditional methods such as the convenience over password memorization, protection against user impersonation and user repudiation but despite the advantages these systems are vulnerable to attacks and poses security risks. The key feature is that the biometric data is preserved and the operations are performed on a unique ID. Hence system offers less vulnerability.

Keywords: biometric, identification, IoT, MQTT, fingerprint

I. Introduction

This article proposes to develop a decentralized biometric solution for identification which is based on IoT and decreases the risk of exploitable vulnerabilities of the proposed system. The proposed solution offers portability, energy efficient design, a distributed secure finger template storage mechanism and an encrypted channel for wireless network communication. The fingerprint templates can also be encrypted if required. The client devices have a localized storage for storing the biometric fingerprint template. The proposed model provides a decentralized biometric storage of data. The key feature is that the biometric data is preserved and the operations are performed on a unique ID. In case of any security threat or attack, the maximum loss will be of 254 fingerprints (on device) which are also encrypted (so less exploitable) and in case of server the loss will be of the numeric IDs and not of biometric data. Hence system offers less vulnerability.

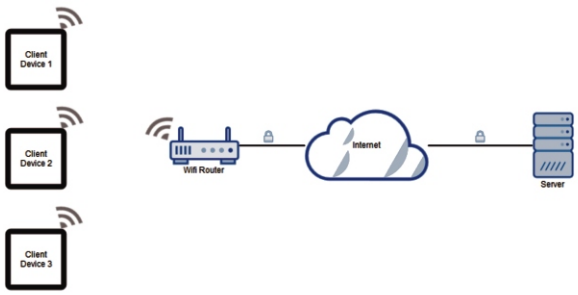

Figure 1: Architecture of the proposed system

Correspondence should be sent to Anand
Assistant Professor, Keshav Mahavidyalaya
University of Delhi, Delhi
E-mail: nanoanand@gmail.com

II. Related literature

The Biometric System: The biometric system for authentication and identification are being increasingly used which are based on human physiology, behavior and chemistry. The universality and uniqueness of the trait in human population is required because the trait which will be used for authentication must be present with each person and should be sufficiently different with each individual. Hence it provides a basis for a valid authentication which is unique to each person. The permanence of the trait is essential so that the trait has a good permanence and is reasonably invariant over time. The good measurability of the trait and its accuracy and speed for the proposed processing is also needed. The used biometric types are iris scan, facial recognition, palm geometry, fingerprinting, and DNA.

The Benefits of IoT: IoT is an internetworking of the physical devices, systems, services, and items embedded with electronics, software, sensors, and network connectivity that enable them to collect and exchange data Madakam, Ramaswamy, and Tripathy (2015). It provides a simplified connectivity between the devices, systems and services. These can go beyond the machine-to-machine (M2M) communications. It also offers a variety of domains, protocols and applications. IoT platform

provides lightweight messaging protocols for communication. IoT allows the objects to be sensed and controlled remotely across the network structures. It creates possibilities for the integration between physical world and computer-based systems, thus it allows for efficiency, accuracy and economic benefits based on the technological connectivity in the world. IoT technology also offers portability and energy design considerations.

The previous models: It is known that the biometric system based authentication offer several advantages over the traditional methods. The advantages such as the convenience over password memorization, protection against user impersonation and user repudiation make biometric system preferable. But despite these advantages these systems are vulnerable to attacks and poses security risks. The possible attack points on the biometric system have been documented by Roberts, Latha, and Ramesh kumar (2013) and Latha and Ramesh kumar (2013). If the biometric data is sent on a centralized server then such database servers are prone and susceptible to disclosure of biometric data which may be irreversible and lost forever.

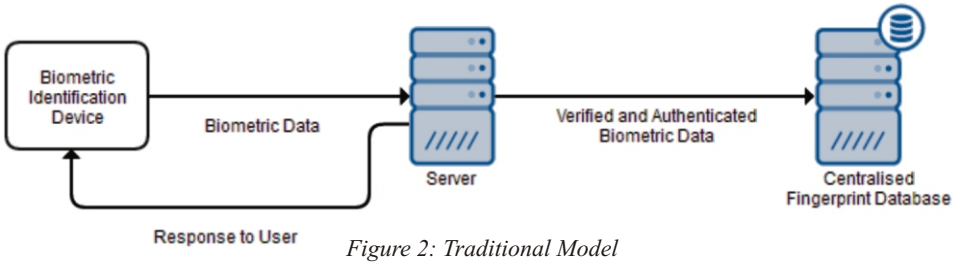

Figure 2: Traditional Model

III. System overview

The proposed system is based on the network backbone of MQTT which is a very lightweight messaging protocol from IoT technology. This protocol uses publish and subscribe model, with a broker as its middle layer. The publisher publishes a message under a topic to the broker and the subscriber subscribes the same topic through the broker. Through this communication channel the data can be sent from one client machine to the server. The IoT technology is typically composed of a sensor to capture the biometric data, microcontroller to handle and process the data, a Wifi module to provide a wireless network communication channel. On the server end the proposed system uses Microsoft .NET framework which uses M2MQTT library to communicate with the broker. The received data from M2MQTT can be further used for storing in a database. The client machine is composed of the following components.

MQTT protocol: The Message Queue Telemetry Transport (MQTT) is an ISO standard public-subscribe based lightweight messaging protocol. It is designed to support wireless networks with varying levels of latency (due to bandwidth constraints or unreliability of the connections). It is a publish/subscribe messaging model facilitating one-to-many distribution. It is ideal for low-powered/battery powered device which ha s a high constraint on power. The header size in MQTT is very small, just 2 bytes which keeps the network utilization minimal.

Fingerprint Module: Synochip AS601 is used which is a member of Synochip CORDIS 5+ family having a 32 bit RISC core. It is used for fingerprint identification and can be used in a wide range of embedded applications. It uses the non-volatile Flash memory for storing the fingerprints. It features SEA (Symmetric Encryption Algorithm) / RSA accelerator engine. The network communication and the stored template both can use encryption. The fingerprint module uses SEA/RSA accelerator engine to implement the encryption and the Node MCU offers secure network communication through SSL/TLS.

Arduino: Arduino is an open source hardware based on ATMEL microcontroller. It consists of both a physical programmable circuit board which is called a microcontroller and an integrated development environment (IDE) used for developing and uploading the code to microcontroller board. This solution uses Arduino to communicate with the fingerprint module over a serial channel to enroll, delete and read the fingerprints. The solution uses modified Adafruit fingerprint library developed by Adafruit industry for the aforementioned operations. A 16x 2 display (is connected with Arduino) is used for printing the output and status of the performed operation.

NodeMCU- It is an open source development board which is based on ESP8266-12E module. It uses NodeMCU firmware which has bit, GPIO, HTTP, MQTT, UART and TLS/SSL modules. The microcontroller board integrates the GPIO, I2C, PWM and ADC into one. It can be programmed using the Lua programming language. The NodeMCU is connected with Arduino over a software serial channel. The read fingerprint ID is sent to the NodeMCU from Arduino which is further forwarded to MQTT protocol.

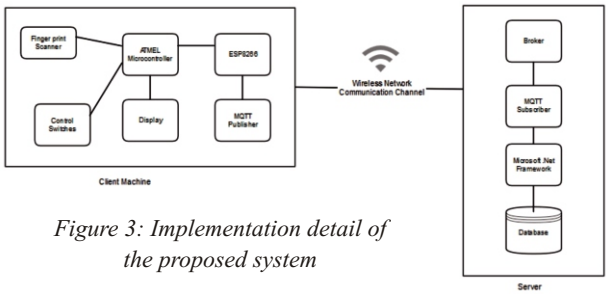

Figure 3: Implementation detail of the proposed system

IV. Implementation

The solution is designed keeping in mind the approach of modularity and extensibility. The client machine has three modes as described below. The identified user ID can be used as per the requirement because the data layer is totally independent of the proposed system. The key feature of the proposed system is the distributed storage of

fingerprint templates in all the client machines (based on IoT technology). Another feature is the portability of the device, as the devices are battery powered and a wireless system which does not need to be mounted or fixed at a specific location. The most important feature is that the biometric data is preserved and the operations are performed on a unique ID. In case of any security threat or attack, the maximum loss will be of 254 fingerprints (on device) which are also encrypted (so less exploitable) and in case of server the loss will be of the numeric IDs and not of biometric data. Hence system offers less vulnerability.

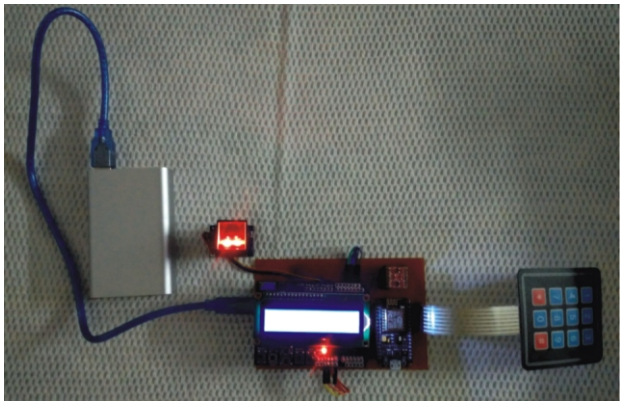

Figure 4: Image of implemented system

The Enrolment Mode: The fingerprint is first of all scanned by the fingerprint module and requests for a unique ID from the user through keypad which is connected to Node MCU. This fingerprint is stored in the memory of the module as a fingerprint template.

The Delete Mode: The solution has implemented the delete mode using the delete function available in Adafruit fingerprint library. The stored unique ID as well as the fingerprint template can be deleted from the fingerprint module by calling the delete mode activated through a micro-switch.

The Read Mode: When activated and connected with network the device waits for a valid finger to be placed on the sensor. The sensor reads the fingerprint and matches with the stored fingerprint template. If the confidence score is above the excepted security threshold then it accepts the fingerprint otherwise rejects it. Once accepted, the fingerprint module triggers the system to forward the unique ID to MQTT protocol. When the system accepts it at the sever end it receives an acknowledgment. Once the acknowledgment is received at the client machine, the user is given the information through a message on the display that the user is identified or not.

The Server End: The server end is implemented using Microsoft .NET technology using C# programming language. The library M2MQTT/GnatMQ, is used to subscribe and publish the messages over MQTT protocol. The ID received at the server is free to be used by the user in possible ways.

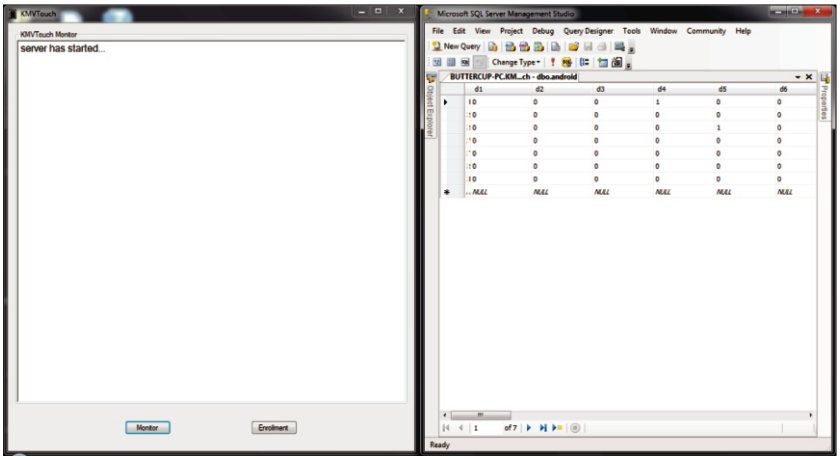

Figure 5: Image depicting Server Application for monitoring the system log (L) and MSSQL server depicting the use of proposed system as an attendance system (R)

V. Conclusion and future scope

The proposed system can have multiple uses because it is portable, easy to operate, wifi connected and power efficient. The network overhead of the system is minimal making it suitable for high bandwidth constraint environment. It is highly secure as compared to the traditional system because the maximum possible attack can damage a single client machine data only. The received ID can be inserted in a database for various applications such as student attendance systems, localized public distribution systems and counting the number of visits etc. The cost involved for the development of this device is very less and it can be manufactured in minimal time. As the solution is modular it can be further modified using other sensors in identification techniques such as iris scan, face recognition, and RFID.

VI. References

[1] Madakam, S., Ramaswamy, R., & Tripathy, S. (2015). Internet of things (IoT): A literature review. *Journal of Computers and Communications, 3,* 164-173. http://dx.doi.org/10.4236/jcc.2015.35021 (accessed on 11 May 2017)

[2] Roberts, C. (2007). Biometric attack vectors and defences. *Computers and Security, 26,* 14-25. doi: 10.1016/j.cose.2006.12.008 (accessed on 22 May 2017)

[3] Latha, U., & Kumar, R. (2013). A study on attacks and security against fingerprint template design. *International Journal of Emerging Trends and Technology in Computer Science (IJETTCS), 2*(5), 13-17. Website: www.ijettcs.org (accessed on 25 May 2017).