A Survey on Authentication for ATM Transaction System

By Osman C. D'silva, Ruthwik H. Param, Samarth S. Kulkarni, K. R. Vadiraj,
Guide: Dr. Amutha S.

Abstract – In this paper, we proceed to discuss the various implications and concepts related to the hardware and software used in our proposed system of fingerprint authentication for ATM card transactions.

This paper refers to many different sources based on the techniques that are being used in the system, i.e. a RFID scanner, RFID tags, a Fingerprint scanner, the Adafruit library and RESTful APIs.

I. Introduction

Authentication is defined as the testing and verification of the asset. The asset can be anything such as a computer IP, a human user, etc. Authentication is mainly used as a security measure for identifying personnel, carbon dating, forged documents, etc.

There are various fields in which authentication is utilized. In the field of art, the authentication of the art piece or artifact is done by verifying the quality and date of the artifact or art piece. In the field of computer technology, it is used to certify a human user to a certain system to allow them into a confidential system or data.

Authentication using biometrics is a majorly used technique for security purposes that involves the physical biometrics of the human user. Biometric hardware captures the biological features of the human, for example, iris, fingerprint, facial recognition, etc. This method is carried out via the cross reference of the received data and the data that is stored in the database. Only if the input data and database values are the same, only then will access be given to the user. This type of authentication is mainly used in the entry ways of corporate building, a means of signing in to a system, etc.

The data obtained from fingerprint recognition hardware is unique as every individual has a different fingerprint. The fingerprint of each human is varied as each individual does not contain the same pattern. This enables the fingerprint recognition system to one of the most protected utilized across the world.

In today's world, the security and privacy of companies and individuals is of great value and it is highly sought after. Authentication offers a higher level of assurance that their data is protected from attackers and illegal users.

The literature that will be touched upon in this survey deals with the various methodologies involved in the making a ATM transaction system using

Fingerprint Authentication and the various libraries that are being used to implement this particular system. It deals with a fingerprint scanner, RFID scanner, RFID tags and the two libraries, Adafruit and RESTful APIs, which will be used to implement the final product.

II. Hardware and Software Methodologies

A. Hardware used

1. Fingerprint Scanner

The paper [1] presents a model to develop a multilevel security system. The primary levels include Hex keypad, RFID & Bluetooth. To get to the secondary level which consists of the final authentication i.e. Fingerprint scanner we need to clear the priori. The primary level security measures are connected to a controller while the fingerprint system is connected to a microprocessor with a separate power supply.

It consists of a R305 finger print module. To access the valuable item only top officials with fingerprint access has to be scanned. Supply voltage of3.6-6.0 VDC with 120mA max current. Use secure TTL to interface with the web. [1]

The pressing biometric problem here is to find a biometric mean to identify infants cheaply, reliably and automatically. Physical traits of infants are tiny, delicate and grow rapidly. The author focuses on novel area of friction ridge skin as the potential answer. IRS algorithm is a global level characteristic of a ridge skin that varies across any area of ridge skin and across the body. It depends on gender ethnicity and age but distinctive enough to broadly classify individuals from a wide variety of the same population.

The Image Quality Algorithm EVA EV algorithm is based on image features extracted from captures of adult fingermarks and a ground truth. For best results a classifier is trained on the scanner images and its parameters are chosen via the lowest error at a fixed rate for the camera and phone images. This classifier employs various support vector machines and k-nearest neighbor algorithms. [2]

Widespread use of fingerprint scanner can be seen in tablets and smartphones coupled with security and ease of use provided by the means of biometric authentication. It is difficult to obtain the performance metrics due to the form factor of the embedded sensors in these devices. The drawback of these sensors is that it captures pixelated biometric data due to the small size of the sensor.

The data obtained from experiments suggests that each individual generates around 300 different biometric images.

Three cropped databases of 10x10mm2 ,12x12mm2 and 8x8mm2 are used. This data was processed using 2 different

algorithms, namely NIST (National Institute of Standards and Technology) and the other is a commonly used commercial algorithm. Cropping of the input images results in degradation of the image quality.

The paper studies two different scenarios, first scenario includes capturing biometrics from the scanner embedded in the device and the second from an external scanner for enrolment. Full size images and the cropped images were compared to analyze the results.

The study shows that both have similar effects. The final results suggest that embedded sensors on devices reduce the quality of the scanned image than compared to the external biometric scanners which is greater in size.

Furthermore, the results depend on the type of scanners and algorithms used for enrollment and authentication. The performance of the commercial algorithm shows a higher efficiency than the public algorithm. [3]

The use of fingerprint identification is widely used for personal and personnel verification to allow for entry to a building or entry to a system. A fingerprint contains a pattern unique to each individual which is never the same for any two humans, even twins. The reason why fingerprint recognition is highly revered is due to the fact that each human has a unique fingerprint.

Since the technology used to implement an authentication system using fingerprint is highly sought after in modern times and hence making the such systems quite expensive. Nowadays the price for a basic fingerprint scanner ranges between RS. 1000 to RS. 2500.

The data obtained from different scanners varies as different companies might use a distinct algorithm or encoding to capture the fingerprint data.

We plan to implement this system of using fingerprints for authentication purposes.

2. RFID

RFID uses radio frequency waves to interact with the RFID tag. The RFID tag gets activated only when the RFID scanner is nearby around 10 to 20cm. The commercially available RFID tag are not very flexible and this effects the durability. This paper talks about how more flexible textile-based RFID tag can be implemented. The commercially available RFID tag antennas work in UHF (Ultra High Frequency) spectrum range. This spectrum range is defined from 952 to 954 MHz. The widely used high-powered systems using a passive tag can use an antenna whose power is between 10 mW to 1 W and an antenna gain defined by the power transmitted by the antenna in a particular direction can be of 6 dBi.

The more flexible version of the RFID tag antenna is built for implementing with elastic material for example automotive tires. The designed tag uses a profile which is low in structure so that the complexity of integrating and building cost is reduced. The elasticity provided by this type of flexible tag can help in operating in hostile environments where they may be subjected to deformation. The tag designed has better read ranges than the ones implemented using copper wires, this is due to the fact the new tag is fabricated by embedding the RFID tag in a polymer. By using a flexible and textile based RFID tag antenna it was demonstrated that the antenna achieves a bandwidth of 263MHz in free space and it also maintains its tuned behavior when the tag is placed in dielectric medium. The performance of the designed tag was also observed and it was concluded that the tag does not degrade under mechanical deformation up to 10%, which good evidence that the tag can handle hostile environments. [4]

RFID tags are used in widely for tracking objects and shipments. The real time location of the object using the RFID tag is difficult to obtain as the tag needs to be in active mode always. The location information using a passive tag in implemented in this paper. Many papers have been written which uses the k-nearest neighbor principle localization systems for passive RFID tags. These systems used the RSSI (Received Signal Strength Indicator) at the reader and compare it with different RSSI of the reference tags.

The RFID localization system used here rely on phase evaluation of the tag response signal. This evaluation is represented using the term phase of evaluation (PoA). A multiple input multiple output system is designed which consists of each frontend is configured to work as transmitter and the remaining frontend is configured to work as receiver. The measurements were carried out in an indoor office. A 2D representation of the position measurement was demonstrated for the passive RFID tags based on PoA evaluation of the signals. The ambiguity in the phase measurement is handled by arranging tags in a uniform linear array to simultaneously estimate its position. [5]

In this paper [6] the localization of the RFID is based on evaluation of backscattered tag signals. By combining phase and amplitude evaluation the accuracy and the robustness of the estimation of tag position if improved compared to the approach of using either one of them. The passive RFID transponder which is used to estimate the position of the tag communicates its information by means of backscatter modulation, where the reflection coefficient of the tag antenna is switched

between two stages in accordance with the data being sent. Hence the localization can achieve based on PoA and amplitude as these parameters rely on the position of the RFID transponder. Furthermore, the algorithm used here does not rely on reference transponders. [6]

The main drawback of using an RFID sensor is that the range for detection is very small, usually around 5-10 feet and sometimes up to 15 feet. However, there is a bypass to this limit or constraint. The effect of quantum tunneling can be exploited to increase the range of an RFID tag to close to 300 times the usual range. This RFID tag works on a 5.8GHz band. The most impressive characteristics of this backscattering would be that it has a return gain as high as 35dB and sensitivity of -81dBm. It also is very power efficient consuming very little energy.

This is impressive for many reasons; one is the major application that it can see in Internet of Things. Secondly, this is also one of the main tools to pick up card details from unsuspecting by passers. RFID chips are very frequent today on credit and debit cards which would make this improvement a massive advantage for anyone who would intend to skim a card from farther away.

Even though there are no RFID frauds reported, it could open up a world of possibilities in the future for threats and major fraudulent activity with this. [7]

RFID technology works on 2 main components, namely RFID Scanner and the RFID tag. The information is stored on the tag while the scanner is responsible for reading the information of the tag. When the scanner reads the tag, there is information exchanged between the scanner and the tag and this is when the details are at risk of being intercepted. This is a major breach in privacy since it contains half of the details required to access any credit or debit cards, the other half being the PIN, 2FA or biometric authentication. Through this information there are many ways to figure out more personal information about the card holder as well as get the PIN through social engineering.

Since RFID works on low energy consumption, it is advantageous to have a protocol that is as lightweight as possible, hence the protocols which experimentally satisfy privacy and lower power consumption are preferred in many fields including, but not limited to, IoT and cybersecurity. [8]

We can calculate and estimate a 3D position of a RFID tag by obtaining the three co-ordinate measures. This allows to track the movement and could possibly lead to detecting suspicious behavior inside or around ATM stalls or vestibules. This allows another potential security feature. The main challenge for this

proposed solution would be the estimation of location precisely without consuming a lot of computation power. To bypass this restriction, we can outsource the computation to a computer outside the stall or vestibule for calculation of the distance. The only sensors inside the ATMs would be utilized for obtaining the co-ordinates of the tag.

This can also be utilized to inform users via a text message if and when they leave their card behind in the ATM. The solutions 3D positioning of RFID based on ultrasound provides are numerous and it is also applicable in many fields such as IoT applications and banking sectors etc. [9]

A RFID scanner is a device that uses radio-frequency waves to wirelessly transfer data between itself and a RFID tag in order to identify, categorize and track assets.

The RFID scanner works in accordance with the RFID tag which is a small sticker or a chip on a card, with relation to our system, and it contains electronically stored information which the RFID scanner will read via radio waves.

We have discussed the various types of RFID and the concepts relating to RFID. We have chosen to adopt a few of the ideas and concepts into our projects as they pertain to exactly what we require to be done in our system.

B. Softwares

1. RESTful APIs

REST stands for Representational State Transfer which is a software architectural style that defines a set of constraints to be used for creating Web services. Any web service that complies with the REST architectural style is called a RESTful Web service and this provides interoperability between computer systems on the internet. REST is a lightweight replica to mechanisms like Remote Procedure Call (RPC), etc. RESTful APIs can be used for service composition, a well-used structure to coordinate distributed services by imposing constraints. The paper deals with testing of the various composite services provided by RESTful APIs and their performance in accordance to the assorted databases available.

The method in which the RESTful APIs are to be implemented in the design is such that the user is able to understand exactly how an ATM transaction occurs in real life with Fingerprint Authentication as a verification method, as an alternate to the generic PIN that users already utilize. The RESTful APIs will help in integrating the system onto a web-based application which uses the following languages: HTML, CSS, JavaScript, Node.js, Express.js and MongoDB as the database in which all the information of the user is stored. The APIs will help in creating a viable website in which the transaction of

a user can be viewed and the authentication process is also done. [10]

RESTful APIs in this project are mainly used to represent exactly how the transaction would look like as majority of ATM transactions are done in the backend and the end user doesn't see any of the authentication process.

2. Adafruit Library

The Adafruit library is a library that can be used for fingerprint sensing in an Arduino board or a fingerprint scanner. It can be used in various ways like pressure sensing, weather monitoring sensing and so on and that is what the paper discusses. The method in which the Adafruit library is used in the paper is related to an IoT aspect of climate monitoring using a Raspberry pi and the method that we plan to implement the Adafruit library is through a fingerprint scanner for our ATM transaction system which uses Cyber Security for its authentication for the transaction. Even though the implementation of the Adafruit library differs on the two projects but the methodology in which the library is implemented is more or less similar in nature.

The paper discussed developing an IoT system that will allow the quality of life to the people to increase by providing a clean and sustainable environment. The authors discuss about the various components that will be used in their system and the various architectures that will be used to implement such a system. In the paper, the authors have decided to use the Adafruit library as a means to allow client-server communication, which is exactly how we plan to utilize the library but here, in the paper, the authors have used it to publish output to the whichever user has subscribed to it. The authors offer a simple, low cost, low power consumption to a problem involving the environment and we plan to implement the exact same concept but in terms of a fingerprint scanner and the authentication it can provide to the user while he or she accomplishes a transaction on their account. [11]

The concept which is shared in the paper is what we wish to follow for client and server communication by allowing the user to utilize his or her fingerprint to notify the server that the user belonging to that account is conducting a transaction and the server can authenticate whether or not the user in the terminal is the same user in the database via the user's fingerprint. This allows for a more secure system of transacting in a bank's ATM.

This paper [12] deals with the design and implementation of a finger based lock system for shared access of a door system. The paper deals with an Arduino UNO component linked to a fingerprint scanner which controls the door lock.

Biometric systems such as fingerprint provide tools to enforce reliable logs of system transactions and protect an individual's right to privacy. The RFID or password based door lock mechanisms can easily be compromised when the RFID card or passwords are shared or stolen, thus for facilities with shared access require biometric based secure system. In the proposed system, fingerprints of the authorized users are enrolled and verified to provide access to a facility that is used by multiple users. A user can also be removed and a new user can be enrolled in the system.

The paper fails to deal with the issue of multiple electronic locks and that the end product is quite bulky and so the paper also discusses how the entire system can be improved via Multi-locks, Computerized Fingerprint lock system, Smartphone based fingerprint authentication and so on.

The limitations of this product that this paper states are that the scanner will not be able to detect any fingerprints if the fingerprint has been exposed to any chemicals or damaged. It also cannot deal with dirt particles on the finger as well as any cuts or bruises that show up on the finger of the user. The system implemented cannot also correctly detect the fingers of children due to the constant growth that children go through. [12]

III. Conclusion

The project that is to be implemented will be focusing on the various methodologies and libraries that have been detailed in the survey. It has been discussed about the various applications of the different techniques that are going to be used in the design and exactly how these techniques are to be implemented in relation to the project. The libraries that are to be implemented are also discussed in length, the different ways in which the libraries will be utilized in the design.

Using the various literatures, it can be seen what exactly the various methodologies and libraries play what part in the design and how implementation will make the difference in the design.

The design is building on the various theories and concepts brought out by the literatures and by building on said theories and concepts, the implementation of the various techniques and libraries will help in the final design.

IV. References

1. Goyal, Sanket, et al. "Multi-Level Security Embedded With Surveillance System." *IEEE Sensors Journal*, vol. 17, no. 22, 2017.
2. Kotzerke, Johannes, et al. "Steps to Solving the Infant Biometric Problem with Ridge-Based Biometrics." *IET Biometrics*, vol. 7, no. 6, 2018.
3. Fernandez-Saavedra, Belen, et al. "Small Fingerprint Scanners Used in Mobile Devices: the Impact on Biometric

Performance." *IET Biometrics*, vol. 5, no. 1, 2016.

4. Shao, Shuai, et al. "Broadband Textile-Based Passive UHF RFID Tag Antenna for Elastic Material." *IEEE Antennas and Wireless Propagation Letters*, vol. 14, 2015.
5. Scherhaufl, Martin, et al. "Robust Localization of Passive UHF RFID Tag Arrays Based on Phase-Difference-of-Arrival Evaluation." *2015 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, 2015.
6. Scherhaufl, Martin, et al. "UHF RFID Localization Based on Evaluation of Backscattered Tag Signals." *IEEE Transactions on Instrumentation and Measurement*, vol. 64, no. 11, 2015.
7. Amato, Francesco, et al. "RFID Backscattering in Long-Range Scenarios." *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, 2018.
8. Fan, Kai, et al. "Cloud-Based Lightweight RFID Healthcare Privacy Protection Protocol." *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016.
9. Carotenuto, Riccardo, et al. "*Ranging RFID Tags with Ultrasound*." *IEEE*, 2018.
10. Sakthivel, Usha, et al. "RESTful Web Services Composition & Performance Evaluation with Different Databases." *2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, 2017.
11. Shete, Rohini, and Sushma Agrawal. "IoT Based Urban Climate Monitoring Using Raspberry Pi." *2016 International Conference on Communication and Signal Processing (ICCSP)*, 2016.
12. Baidya, Jayasree, et al. "Design and Implementation of a Fingerprint Based Lock System for Shared Access." *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 2017.