

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IMPACT FACTOR: 7.056

IJCSMC, Vol. 13, Issue. 5, May 2024, pg.107 – 115

Fingerprint-Enabled ATM Network

Pragati Agrawal¹; Rohan Saxena²; Saksham Agrawal³; R.K. Singh⁴

^{1,2,3,4}(Department of Mechanical Engineering & Delhi Technological University, India)

¹ pragati1234ag@gmail.com; ² rohansaxena858@gmail.com;
³ agrawalsaksham1323@gmail.com; ⁴ rohansaxena859@gmail.com

DOI: <https://doi.org/10.47760/ijcsmc.2024.v13i05.011>

Abstract: Large data collections are stored by people in the modern world utilizing computers. Data may be sent across the globe at a reasonable cost. ATM's have been in use for almost 50 years now since their introduction. Since its introduction, ATM's have made it possible to withdraw money without encountering any problems. In the banking industry, the ability of ATM's to be installed in any location is seen as exceptional since it allows customers the freedom to conduct transactions on their own. While the cash dispenser and visual screen serve as output devices, the card reader and keyboard serve as input devices. Many ATM's can work together on a common level through the host processor, which is owned by the bank. Authenticated Banks provide unique ATM PINS to their customers. The registered phone number is used to send these ATM PINS. if someone saw the PIN notice on the user's phone and knows the card data. They can then access the client's account in full and may be held accountable for any criminal activity that occurs. Criminals have developed a variety of schemes to steal money from ATM's. Due to strict security measures around the money compartment, they are unable to simply steal cash from an ATM; instead, they swipe the cards of several customers. It is far easier to obtain ATM card data than to breach the ATM's security. The practice of card skimming is one that con artists frequently employ. On the card per user space of ATM's, card skimmers are implemented. The data is stored in the memory of the card skimmer and is seen by an electrical circuit on a visually appealing portion of the card. After driving the skimmer out of the ATM, the criminals later duplicate this data. Card skimmers are designed to fit perfectly over each user's unique cards, making it easy for clients to become victims of them.

Keywords: OTP, Database, SQL, NOSQL, PIN, URL

I. INTRODUCTION

Our goal is to introduce a potent technique that uses fingerprint sensing to enhance the current state of ATM's. It is widely acknowledged that each person has a fingerprint that is distinct from everyone else. Thus, we will lessen the likelihood of thefts occurring in the present day, since the offenders can access systems through technological means and obtain all of the user's private information, but they will be prevented from completing the transaction if the fingerprint is not authenticated. In order to undertake operations only after a comprehensive validation of the user's fingerprint from our database, we are additionally incorporating One Time Passwords that are sent via the registered user's phone number and email address as ATM PIN. Criminals have developed a variety of schemes to steal money from ATMs. Due to strict security measures around the money compartment, they are unable to just take cash out of ATMs; instead, they swipe the cards of various customers. It is much easier to steal ATM card info than to breach directly into the ATM. The practice of card skimming is one that con artists frequently employ. On the card per user space of ATMs, card skimmers are implemented. The data is stored in the memory of the card skimmer and is seen by an electrical circuit on a visually appealing portion of the card. After driving the skimmer out of the ATM, the criminals later duplicate this data. Card skimmers are designed to fit over unique cards perfectly making it easy for customers to become victims of it. In the unlikely event that card spaces appear large or unrestricted, it may be a skimmer device. Additionally, fake key cushions that log all customer inputs are available online from obscure web commercial centers. These can be placed over the ATM's primary key cushion.

Then, thieves take advantage of these logged inputs to withdraw money from the client account. Additionally, thieves can place a tiny camera directly above the ATM keypad, which keeps recording customer inputs, including your PIN. Banks frequently advise their customers to shield the keyboard with their other hand when accessing the PIN. Occasionally, the entire front of the ATM is replaced with a false one that exactly mimics the original. It turns out to be challenging to determine whether an ATM has been compromised in the event of a phony ATM front. Money doesn't flow out of the fake front, and customer inputs are still being recorded.

II. OVERVIEW OF FINGERPRINT AUTHENTICATION

- Step 1 Registration: The registration process involves first detecting the user's fingerprint, processing it into a digital image, and then purging any undesirable features from it. After post- processing, store the image in the database.
- Step 2 Authentication: To operate on a fingerprint, we used a fingerprint sensor. It extracted features from the fingerprint and compared them to N fingerprint templates stored in our database.
- Step 3 Confirmation: After a fingerprint was found to match a specific fingerprint in our database, we double-checked the match by comparing the fingerprint to the database once more.

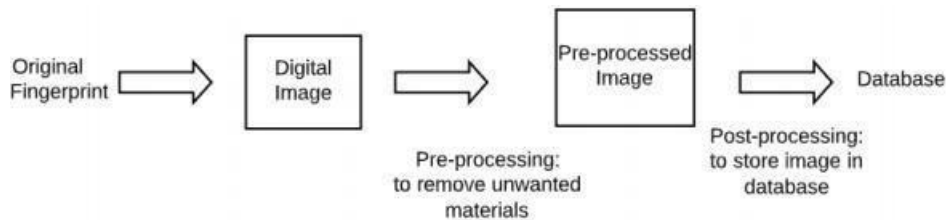


Fig. 1 Registration

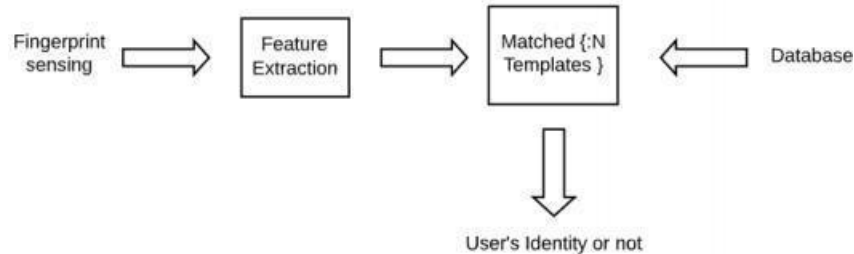


Fig. 2 Authentication

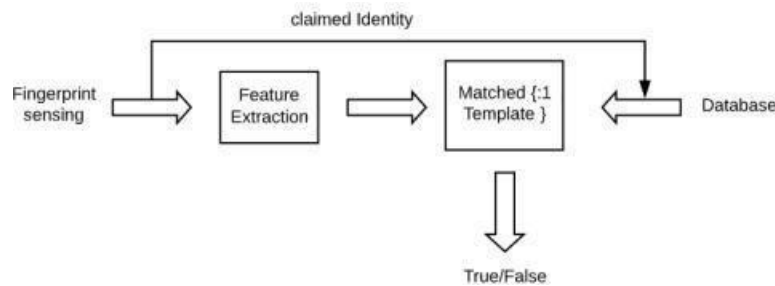


Fig.3 Confirmation

In addition to fingerprint recognition, the matching fingerprint customer's registered phone number, 99XXXXXXX, and registered email address, customeruser@example.com, will receive three One Time Passwords. By all means, he can complete transactions if he can accurately enter the OTPs on or before the third OTP is transferred.

He will have to start the process over if the amount he inputs to be withdrawn is more than what is already in his bank account.

After the transaction is complete, he will get an email and a text message on his phone saying that the transaction on this account number, 56XXXXXX, was successful and that the remaining amount is what he needs to pay. Conversely, following the collapse of the third OTP, he will get a security breach alert email and be instructed to get in touch with the closest branch right away.

Face recognition problems are one way to counteract the existing state of affairs. As a result of biological ageing, the characteristics of a person's face become increasingly out of proportion from the last picture they had taken. For the device to remain productive, the user must periodically re-register their image, which could be extremely difficult for a bedridden patient or someone who has had their face burned. Comparing biometric IDs to more conventional and contemporary approaches has several advantages. Installing it is fairly easy, although it does require some time and effort to locate each finger and fingerprint scanner. Because of this, fingerprint recognition is regarded as one of the easiest biometric verification methods to use.

A webcam was mounted on the ATM, according to [23], and it records the clients' live photos as they pass by. After then, this taken image is compared to the other pictures in the database. An arbitrary password is generated by the contrast and sent to the client's registered phone when it is successful. The customer is then directed to input the identical password on the ATM's screen. The user can carry out transaction actions if they input correctly. However, there are two significant problems with this theory: 1) Unless prompt action is done, it will be impossible to stop theft from occurring if the mobile phone is lost or stolen. 2) The initial image was created because as we age, our face expressions tend to alter. There will be differences between the picture of our faces that was taken at that time and the most recent one.

According to the researchers, the idea of using the PIN as a secure password is not very suitable for the ATM's Palm Print Recognition and Confirmation System [4]. Thus, the idea of fingerprint authorization was established in order to increase security. According to extensive research, a simulator mimics the features of the ATM as it exists today. They compared the cervical recognition program's 89.43% rejection rate to 10.57% in their conclusion [4].

As a result, 53 out of 500 users who visit the updated ATMs after going through this verification procedure may experience issues. The percentage of rejections was increased to ten percent.

To eliminate errors in ATMs' alphanumeric certification, Lalzirtira implemented Graphical User Authentication. His research indicated that an image-integrated code would be easier to understand. He devised a password that would be simple for customers to commit to memory [5]. Although the pass-code that uses photographs to grant authorization in the ATM system has some benefits of its own, it was unsuccessful because of video recordings.

Dyno-password idea was another one that was proven to be true. Here, the bank sends the client a text message on the registered phone number, which contains the passcode. The ATM screen will be used to input this new passcode. The bank's database server will cross-check it once more. It follows that all that is required to withdraw cash from an ATM is the customer's PIN, card, and SIM. This kind of sensitive information can be readily obtained by anyone in the client's social circle. This idea thus provided opportunities for hackers [6].

III. SOFTWARE

A. *Mongo DB*

An open-source record database with excellent performance, high accessibility, and designed scaling is called MongoDB. To put it simply, Mongo DB is a database that is oriented towards records. It is an open-source product that was developed and supported by 10gen. MongoDB can be accessed for free under a general public licence, and it can also be accessed with a commercial licence from the creator. "A document-oriented database system that makes advantage of the NoSQL notion is called Mongo DB. It also offers automatic scaling, great performance, and high availability. This open- source application was created and is maintained by 10gen, a company that was founded in October 2007. MongoDB is a free database management tool offered under the General Public Licence (GPL) and Commercial licence issued by the producer. It was also planned for MongoDB to run on commodity systems. MongoDB is the database of choice for businesses of all sizes and in all sectors worldwide. A database in MongoDB can be thought of as a physical space containing various types of data. Every database has a live assortment of documents here on the record framework. A MongoDB server often houses a number of databases.

B. *Python Spyder*

Like Perl, Ruby, Scheme, or Java, Python is an object-oriented programming language that is powerful and easy to understand.

Among Python's noteworthy attributes are:

- Its elegant syntax makes your programme easier to read.
- The language is user-friendly, making it effortless to get your programme up and running. Because of this, Python is perfect for a variety of ad-hoc programming tasks, including developing prototypes, without sacrificing maintainability. It has an extensive standard library that supports a wide range of common programming tasks, including connecting to web servers, using regular expressions to search text, reading, and editing files, and testing brief code snippets with ease. Additionally, there is the IDLE packaged development environment.
- Easily expandable with the addition of new modules written in compiled languages like C or C++.
- It is compatible with Mac OS X, Windows, Linux, and Unix, and there are unofficial builds for Android and iOS as well.
- Free software is defined in two ways. The cost of downloading, using, and incorporating Python into your programme is zero.
- Despite being protected by copyright, Python is freely modifiable and re-distributable due to its open- source licence.

C. *Tkinter*

There are several solutions available in Python for creating a GUI (Graphical User Interface). Tkinter is the most widely used approach of all the GUI methods. It is a typical Python interface to the Python-bundled Tk GUI toolkit. The quickest and most straightforward approach to construct GUI apps is with Python and Tkinter. Using Tkinter to create a GUI is a simple process.

Making a Tkinter application:

- Bringing in the Tkinter module
- The process involves creating the main window (container), adding any number of widgets, and then applying the event trigger to each widget.

D. *Visual Studio (Node JS)*

Node.js provides a framework for developing efficient and expandable server applications utilizing JavaScript. Acting as the runtime environment, Node.js is complemented by npm, which serves as the package manager for Node.js modules. Visual Studio Code comes pre-equipped with built-in support for both JavaScript and Typescript languages, along with debugging capabilities for Node.js. However, for executing Node.js applications, it's essential to have the Node.js runtime installed on your local machine. This runtime facilitates the execution of JavaScript code outside the browser environment, enabling the development of diverse server-side applications with ease and efficiency.

IV. PROCEDURE

The process via which fingerprints are recognized:

Biometric fingerprint technology is the most widely acknowledged security mechanism to be placed in the ATM. Compared to the current ATM security; it offers a considerably more secure initiative. Because it is so simple to install and use, the technology's ability to blend seamlessly with our modern lifestyle is astounding. It is praised as one of the most effective authentication methods as a result. Since the fingerprint data are not kept in a database, there is no way for the fingerprint to be misused.[7]

Two essential presumptions underpin the unique finger impression ID: peculiarity and in-variance. Constancy. According to in- variance, the characteristics of the finger impression don't alter throughout time. Peculiarity: suggests that the one-of-a-kind mark is remarkable and no two people's distinctive finger impressions are alike.

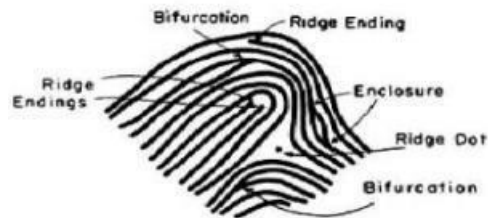


Fig. 4 Fingerprint characteristics [1]



Fig. 5 Fingerprint Types

- Distinctive biometric impression: The biometric's component example is its distinctive pattern. [21]
- Binarization: This refers to the process of converting a greyscale image into a binary image by determining the esteem value. [21]
- Block Filter: This technique effectively extracts minutiae by reducing the thickness of all ridgelines to a single pixel width. [21]
- Minutiae Extracrtuction: After minutiae are eliminated, details are deduced.[21]
- Minutiae Matching: This compares unique finger impression data. Additionally, the minutiae coordination layout is used. [21]
- Matching Score: This is the relationship used to determine how well the original fingerprint and template data collaborate. [21]

V. APPROACH FOR ATM MODIFICATION

They won't check for a one-time password from the bank using their registered phone number or email ID until their fingerprints have been carefully verified.

Three opportunities will be provided for them to write their accurate OTP in front of the ATM screen. In the event that there is enough money in their accounts, they will be able to withdraw money if they enter it correctly. However, if, despite our giving them three One Time Passwords, they enter them wrong, we will send them an email saying, "Security Breach and Kindly Contact your nearest branch." API's will be used by us for sending and receiving obtain the customer's uniquely identifiable data.

The framework is introduced to carry out specified assignments, like email correlation, phone compatibility, validation of Python code, and so on. Each method is then reset to begin regulations. Because the intended technology includes fingerprint sensing, it differs from the current ATM system. It will start as soon as the customer walks into the ATM. First, it will be indicated if the person wishing to open an account with our bank is an existing customer or a new one. If the person is already a customer, they will be requested to move straight on to the procedure' fingerprint authentication step. Should they choose not to, they will be required to register with us by providing their phone number, email address, and fingerprint in our database.

The pictures of our encrypted database are as follows:

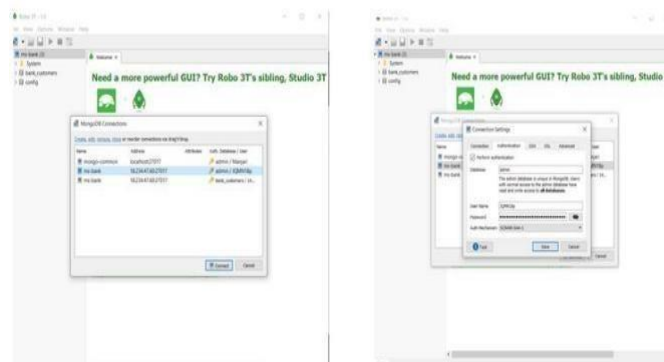


Fig. 6 Database with Password Protection

It indicates that the ability to access the database is restricted to the owner of the verified credentials, such as the admin password. Following that, fingerprints will be requested from both new and current customers in order to confirm their inclusion in our database. As long as their fingerprint scan yields a satisfactory confidence match with our database, they are free to proceed. Their ability to participate in the following phases will be restricted if the fingerprint authentication is unsuccessful. In order to prevent fraudulent activities, it is necessary to ensure that the amount of sensitive information that hackers can readily trace, such as card numbers, personal information security, and mobile numbers, will decrease to the point where people feel safe and secure.

On the successful verification of the fingerprint, they will be asked to enter the first OTP send to their registered Email Address and Phone Number. If they enter it correctly, they will be asked to enter the amount they want to withdraw. If the amount entered is less than the balance present in the bank account, they will successfully withdraw it. On the backend side, we will update the remaining balance in our database. If they fail to enter their first OTP accurately, then a second OTP will be sent to their Email Address and Phone Number again with following the same consequences. On the third OTP, they will have only one chance to enter it fairly. If they failed to do so, then from our side, a security breach mail and a text message will be sent to their registered Email Address and Phone Number, and they will be locked out to proceed for the transaction of money. They have to start over with the whole process again. We are using Python GUI Tkinter as the interface to take the input from the user. We are using API's and Mongo DB to extract and deliver the data of customers on the requirement. We have deployed an online URL for registering using WIFI with us: www.msbank.co.in. This URL is responsible for generating APIs.

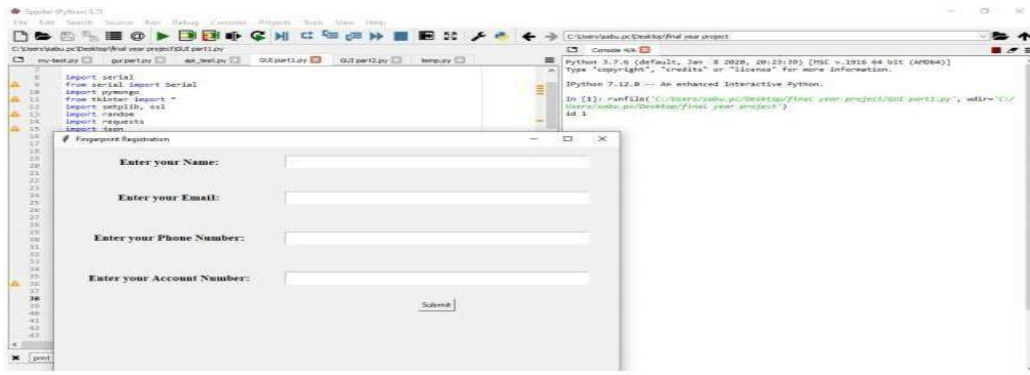


Fig. 7 Illustrates a graphical user interface (GUI) designed in Python for data entry purposes.

VI. RESULTS AND DISCUSSIONS

In this context, we submit the technical input of our research project.

A. Database

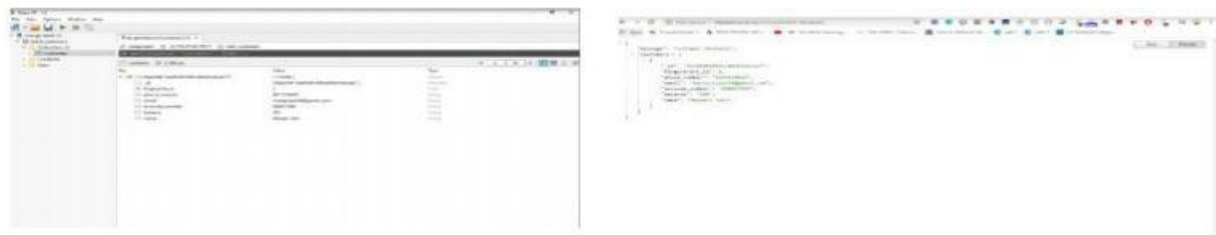


Fig. 8 Our initial database, Mongo DB, is shown in image a) APIs are shown in image b) It displays our database of active MS Bank customers.

B. Updating the existing database by adding a new entry

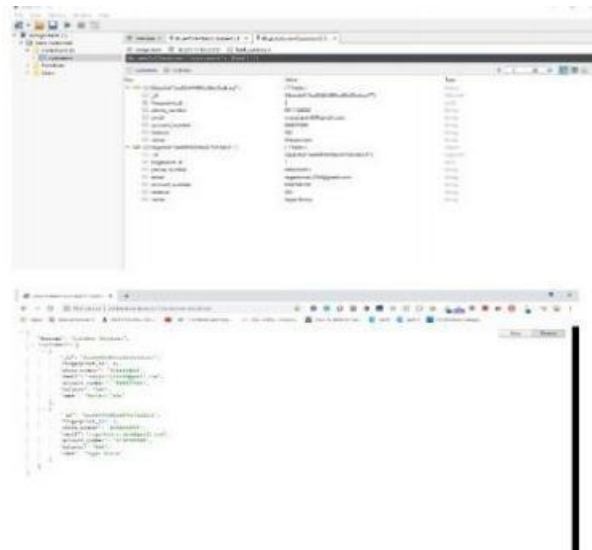


Fig. 9 Shows how the API's are updated with the new user's database in Image b and Mongo DB in Image a. It demonstrates that the new data has been successfully added to our database and API's.

C. Successfully entering the OTP

According to the amount in his or her bank account, it indicates that every registered customer who enters the OTP matching from the texts and emails is permitted to perform transactions.



Fig. 10 Effective Fingerprint Verification (A new GUI displays requesting the first OTP to be provided here after the newly registered user's fingerprint is successfully verified.)

D. Incorrect entry of OTP

This is the situation that arises when a registered customer enters the OTP incorrectly for the third time. They will consequently receive an email titled "Security alert, kindly contact your nearest branch as soon as possible."



Fig. 11 First OTP is incorrect The client inputs the initial OTP incorrectly.(The GUI presents a warning saying "Wrong otp 1" when the customer enters the first OTP, which doesn't match the one sent to the registered Email and Phone No. After that, in order to get the second OTP, the consumer must select "Click to Receive OTP.")

VII. CONCLUSIONS

The existing research on enhancing ATM security through fingerprint authentication, as outlined in the Literature Synopsis, revealed certain inconsistencies. Consequently, there was a pressing need to enhance ATM security with a more effective and cost- efficient solution. The proposed approach involves integrating fingerprint authentication, but with a deviation in the method of delivering OTP's compared to previous studies. OTP's are now sent via two channels: the client's registered email address and phone number. The methodology entails offering new clients the option to register with the bank through a Python GUI (ATM Screen). For registered clients, the ATM Fingerprint Sensor first verifies their biometrics. Subsequently, an OTP is sent to their registered contact details. In the event of an incorrect entry for the first OTP, the client has two additional attempts to input it accurately. If the third attempt fails, the client (or suspected hacker) is barred from conducting any transactions, and a Security Theft Alert email is dispatched. Additionally, the URL www.msbank.co.in facilitates online registrations for clients and the creation of API's for securely storing data of new and enrolled clients. This system ensures that clients can still access OTP's even in scenarios where Wi-Fi is unavailable, by utilizing mobile OTP's, or retrieve lost OTP's from their logged email address. In conclusion, the research findings validate the feasibility of this proposed approach.

ACKNOWLEDGEMENT

With immense pleasure and a deep sense of gratitude, we wish to express our sincere thanks to our supervisor Prof. R.K. Singh, DTU, without his motivation and continuous encouragement, this research would not have been successfully completed. We are grateful to the Chancellor of Delhi Technological University for motivating us to carry out research in the Delhi Technological University and also for providing us with infrastructural facilities and many other resources needed for my research. We like to acknowledge the support rendered by our friends and faculties in several ways throughout our research work. We wish to extend my profound sense of gratitude to our parents for all the sacrifices they made during our research and also providing us with moral support and encouragement whenever required.

REFERENCES

- [1] F. A. Afsar, M. Arif and M. Hussain, National Conference on Emerging Technologies, 2004, "Fingerprint Identification and Verification System using Minutiae Matching", pp.141-146.
- [2] Hmadri nath moulick, Joyjit Patra, Arun kanti Manna, International Journal of Engineering Inventions, Volume 3, Issue 1, August 2013, "Computer Assisted and Contour Detection in Medical Imaging Using Fuzzy Logic", pp-1-7.
- [3] Kavita Hooda, International Journal of Scientific and Research Publications, Volume 6, Issue 4, April 2016. "ATM Security", pp-1.
- [4] Sanjay, S. G., International Journal Of Engineering And Computer Science, 2014, "ATM Transaction Security System Using Biometric Palm Print Recognition and Transaction Confirmation System", pp-5332-5335.
- [5] Lalzirtira, National Institute of Technology Rourkela Mtech Thesis, 2013, "Graphical User Authentication, India".
- [6] Anand, D. A., Dinesh, G. & Naveen, H. D., International Journal of Communication and Computer Technologies (IJCCT), 2013. "A Reliable ATM Protocol and Comparative Analysis on Various Parameters with other ATM Protocols", pp. 192- 197.
- [7] Steve Furber, ARM System-on-Chip Architecture, Second Edition, 2000, ISBN 0-201- 67519-6.
- [8] Ratha, N., Connell, J. & Bolle, R., IBM Systems Journal, Volume 40, No. 3, 2001, "Enhancing Security and Privacy inBiometrics-based Authentication Systems", pp. 614-634.
- [9] Petrlic, Ronald, and Christoph Sorge, IET Information Security, Volume 8, Issue 2, 2013, "Establishing user trust in automated teller machine integrity", pp-132-139.
- [10] Myo, N., International Conference on Education Technology and Computer, 2009, "Fingerprint Identification Based on the Model of the Outer Layers of Polygon Subtraction", pp-201 – 204.
- [11] Journal for Research, Volume 2, Issue 12, February 2017
- [12] Ms. Archana S. Shinde and Prof. Varsha Bendre, 2015 International Conference on Computing Communication Control and Automation, 2015, "An Embedded Fingerprint Authentication System", pp-45.
- [13] Yuliang He, Jie Tian, Xiping Luo, Tanghui Zhang, Pattern Recognition, Letters 24, 2003, "Image enhancement and minutiaematching in fingerprint verification", pp-1349-1360.
- [14] Wei Wang, Jianwei Li, Feifei Huang, Hailiang Feng, Pattern Recognition, Letters 29, 2008, "Design and implementation of Log-Gabor filter in fingerprint image enhancement", pp-301- 308.
- [15] Lin Hong, Wan Yifei, Anil Jain, IEEE Transactions on Pattern Analysis and Machine intelligence, Volume 20, Issue 8, 1998, "Fingerprint image enhancement: algorithm and performance evaluation", pp- 777-789.
- [16] Der Chin Chen, Biometric Systems, Design and Applications, 2011, "Portable Biometric System of High Sensitivity Absorption Detection".
- [17] Subhra Mazumdar, Venkata Dhulipala, San Diego, "Biometric Security Using Finger Print Recognition".
- [18] Anil K. Jain, Jianjiang Feng, Karthik Nandakumar, IEEE Computer Society 2010, 0018- 9162/10, "Fingerprint Matching", pp. 36-44.
- [19] Sowmya Ravikumar, Sandhya Vaidyanathan, B. Thamocharan, S. Ramakrishnan, International Journal of Engineering and Technology, Volume 5, No. 3, 2013, "A new business model for ATM transaction security using fingerprint recognition".
- [20] Jun Zhou, Guangda Sua, Chun hongJiang, Neurocomputing, 70, 2007, "A face and fingerprint identity authentication system based on multiroute detection" pp-922-931.
- [21] Mithun Dutta, Kangkhita Keam Psyche and Shamima Yasmin, American Journal of Engineering Research (AJER), Volume 6, Issue 8, August 2017, "ATM Transaction Security Using Fingerprint Recognition", pp-41-45.
- [22] Zhao, F., Tang, X., The Journal of the Pattern Recognition Society, Volume 40, Issue 4, April2007, "Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction", pp-1270-1281.
- [23] Frimpong Twum, Kofi Nti, Michael Asante, International Journal of Science and Engineering Applications, Volume 5, Issue 3, May 2016, "Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication", pp-503.