2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. June 4-5, 2020

USB Fingerprint Login Key

Rohit Gupta
Amity Institute of Information Technology,
Amity University
rohitgupta10020@gmail.com,

Ginni Arora
Amity Institute of Information Technology, Amity University
garora@amity.edu

Ajay Rana
Amity Institute of Information Technology, Amity University
ajay_rana@amity.edu

***Abstract* - Since centuries fingerprint is the best identification method in everyday life for transaction, unique id, login etc. This paper proposes a model for login designed on the technology of fingerprint recognition with USB as authentication method. The model can also be used to encrypt the USB drive to store some important and confidential files. This paper gives a light on the development of fingerprint key verification model using Arduino nano.**

Keywords- Minutia, USB, Security, Fingerprint, Biometric USB drive, Cryptographic

I. INTRODUCTION

In today's time the common people are facing the problem of identity theft and data breach. This problem is increasing day by day. The fingerprint is used very widely for security purpose, so in this paper, fingerprint is a main aspect to secure the user credentials and their data. A device which is very compact, portable and easy to use in different environments and conditions is discussed further in detail. Its quality makes it very usable products in today's world as a security tool for the user. This Device is based on Arduino Nano, it is a Microcontroller board manufactured by Arduino.cc. These are widely used in robotics.

The proposed model is a prototype of a USB key that can be used to login into user's pc or any online account without the need to type password in the presence of anyone [1]. Since a user can use 10 fingers to set up each finger for an account.

Currently, the technology in USB keys exist works on the passwords, keys and encryptions and are used for login the accounts. Whereas in this proposed model the module is designed uses the technology of fingerprint recognition as authentication method. The model will not only used for login the online accounts, but it can also be used to encrypt the USB drive to store information [5].

The main objective of this paper is to increase the security of online accounts, by introducing biometrics instead of password. The combination of fingerprint with USB can be used without fear to type password in a public place, or worse there can be keyloggers installed on public PC's.

II. RELATED WORK

There is existence of similar keys that use the principle of 2FA (Two factor authentication), that require you to enter the password as well the physical key to login into your account, some of these keys are:

- Titan Security Keys are phishing- resistant two-factor authentication (2FA) devices that help protect high-value users such as IT admins [4].
- The YubiKey is a hardware authentication device manufactured by Yubico [4].

In past, USB disk and encryption module were used in the device [7]. A shell application which works on encryption and decryption based on the proposed model technology [9] was implemented. The model was proposed which consist operating system an USB key and the casing inside in which the fingerprint chip is placed and all the processing is done [10]. The invention was also having an encrypted and secured data storage which is secured using fingerprint identification technology [11].

III. PROPOSED MODEL

This device start with the extraction of minutia (fingerprint) of the user through the sensor, the device will verify the user using the fingerprint of user saved in database and match it with the currently extracted minutia, if the minutia matches then the user will be authorized to proceed and access the data or to auto fill the password of any account according to the preference [7], if not, then a warning will be shown. If the warning is displayed more than five times, then the device will be locked. The flowchart of the working of device is shown in Figure 1.

The steps followed for its functioning are as follows:

Step 1: Configuration This is the first step involved before we can use this key for daily purpose. In this step first user needs configure device i.e. key. Then user will insert the key in the system and configure the user details like user id, password and recovery details in the configuration software provided with the device so that the user details can be recovered in case of a loss or theft, shown in Figure 2 [6].

Step 2: Fingerprint Enrollment In this step user will enter(enroll) all his fingerprint in the key and then write a password associated with it. The password will be encrypted using an onboard algorithm that is not accessibleto outsiders

Step 1 and 2 need to be done only once Now the device is ready for use

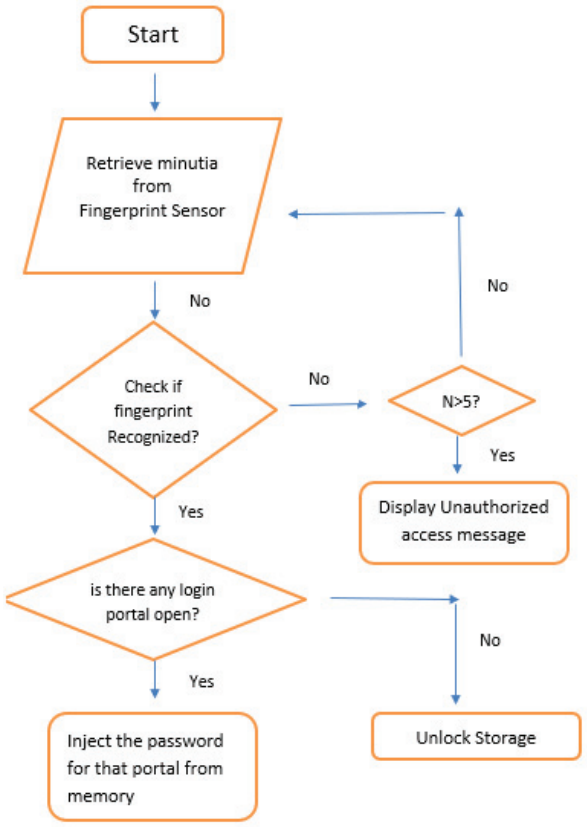

Fig. 1. Flow Chart of proposed device

Step 3: Identification Whenever three is needed to access any of the online accounts, users simply need to enter the login id and use his fingerprint on the device as the password for the account.

Step 4: Authentication and Verification The device will check the authenticity of the provided fingerprint and auto fill the respective password associated with it (if the fingerprint if found to be authentic) [6].

Step 5: Authorization This the final step involved in this system, in this step after the fingerprint identification and verification is done correctly, the user will get the authorization of the account.

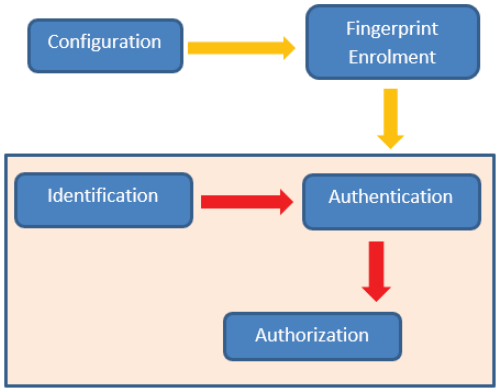

Fig. 2. Block Diagram

A. Internal Functioning

The internal working of the device consists of basic four modules shown in Figure 3 and are as follows:

Module 1: Fingerprint Firstly the fingerprint module extracts the user's fingerprint and sends it to the micro controller for verification. [6]

Module 2: Micro controller The micro controller receives the fingerprint and sends it to the storage module for verification. If the fingerprint is verified, then it authorizes the cryptographic module to autofill the respective password [4].

Module 3: Storage It is used to store the user's enrolled fingerprints, and verifies the fingerprint sent by the microcontroller.

Module 4: Cryptographic It stores the user's passwords in encrypted form, if the fingerprint verification process is successful it decrypts the password and sends it to the micro controller [3].

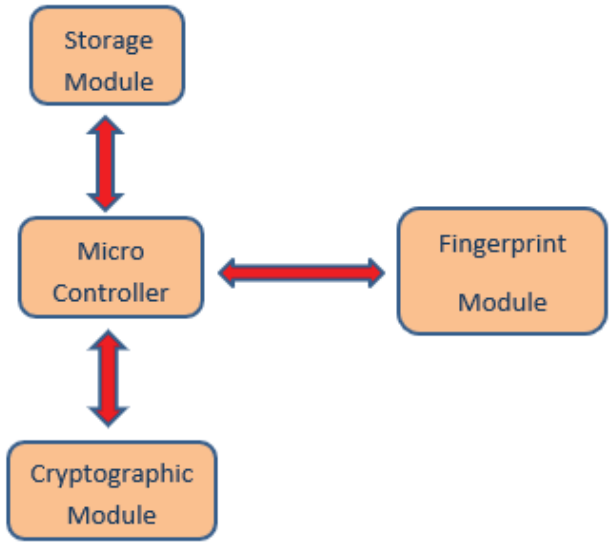

Fig. 3. Internal Functioning

B. Structure of Circuit

This Proposed model has a small USB drive used to store passwords on an onboard encrypted storage, and you can assign each fingerprint to a password for a different account. As soon as you touch the drive with the correct finger the device auto fills the username and password for that account and logs you in securely [1].

The circuit diagram shown in Figure 4 consist of the following components:

- Black wire: This wire connects the pin 29(GND) of Arduino Nano to the ground pin of Arduino fingerprint module and provides a ground connection for power (0 volt).
- Red wire: - It connect pin 30 Arduino Nano to VCC of fingerprint module and provides 5-volt DC for power.

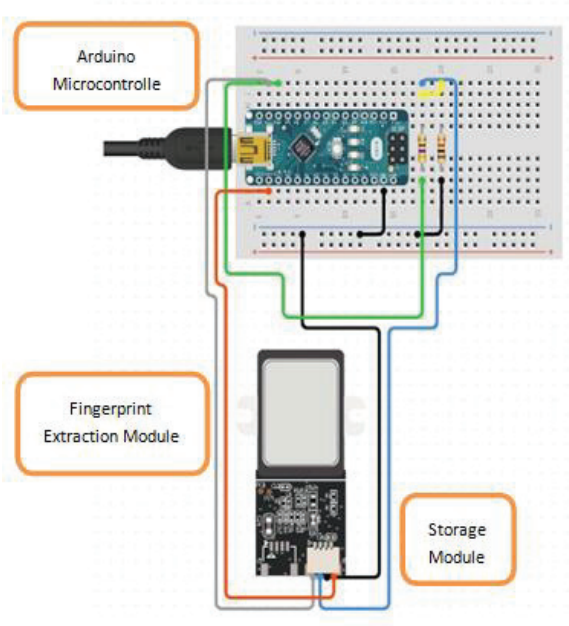

Fig. 4. Circuit Diagram

- Green wire: - This wire connects TX (Transition Pin) of Arduino Nano to RX (Receiving pin of Arduino fingerprint module, it transmits the data from Arduino Nano to fingerprint module [1].
- Blue wire: - This wire connects RX (Receiving pin) of Arduino Nano to TX (Transition Pin) of Arduino fingerprint module, it transmits the data from fingerprint module to Arduino Nano.
- Serial: 0 (RX) and 1 (TX). Used to receive (RX) and transmit (TX) TTL serial data.
- External Interrupts: 2 and 3. These pins can be configured to trigger an interrupt on a low value, a rising or falling edge, or a change in value [5].

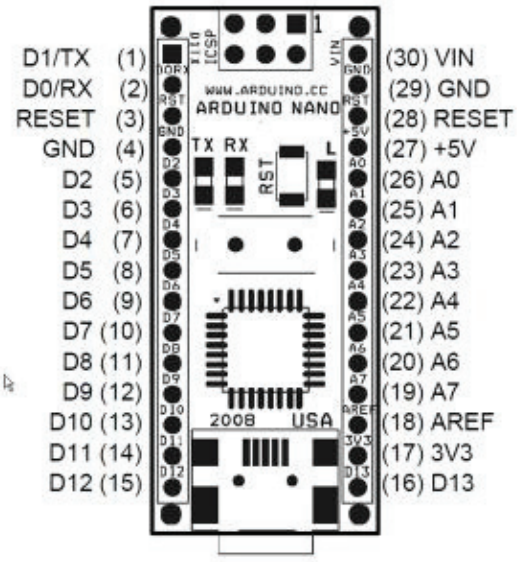

Fig. 5. Pin Diagram

- PWM: 3, 5, 6, 9, 10, and 11. Provide 8-bit PWM output with the analogWrite() function.
- SPI: 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). These pins support SPI communication, which, although provided by the underlying hardware.
- Power: 29(GND), 30(Vin) pins are used to deliver 5v DC power to any attached component. [2]

IV. Analysis and Results

This section deals with the information of tests performed by this device in various conditions and environments and their corresponding result. In order to check the correct working of this device tests has been done many times in different environments. To achieve testing goals of this system, the following components are used:

- Arduino nano
- Arduino fingerprint module
- Storage device

The debugging process is done using Arduino nano. Also, this proposed model has debugged each section of the code to ensure proper functionality thus the step debugging is done.

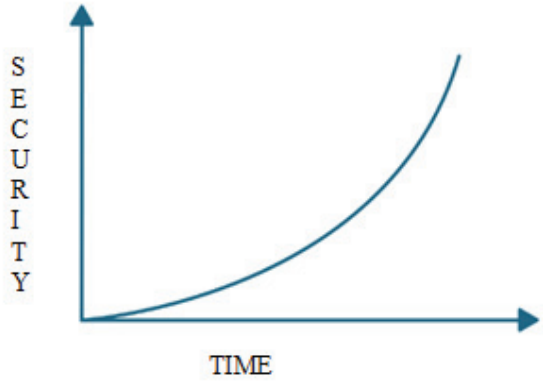

Fig. 6. Security vs Time graph

The Figure 6 shows, with the increase in security the processing time also increase or vice versa, this shows the security is directly proportional to complexity and complexity is directly proportional to time, so in this proposed model moderate security is used to keep the processing faster. This model is a source of energy generation which is efficient and everlasting energy source using the natural resources.

V. Conclusion

The main objective of this paper is to design a device called USB Fingerprint Login key which facilitates user to secure the login credentials and private data. This device will be used to autofill passwords and access stored private data after fingerprint authentication process. In future, further modifications and updates can be made as adding encryption module and fingerprint pattern.

REFERENCES

[1] Lu Yu, Liang Zhong, Yue Chen, "The Research and Application of the Fingerprint Key based USB-Key Pin Number Protection System", International Conference on Information Engineering for Mechanics and Materials, 2015.

[2] Tatsat Naik and Om Sri Satyasai, "FINGERPRINT RECOGNITION", Term paper, https://core.ac.uk/download/pdf/53187952.pdf, 2012

[3] Alper Baştürk ; Nurcan Sarikaya Bastürk ; Orxan Qurbanov. "Fingerprint Recognition by deep neural networks and finger codes" , 5th International Conference on Information Engineering for Mechanics and Materials, 09 July 2018

[4] Kai Cao; Anil K. Jain, "Automated Latent FingerprintRecognition", 10.1109/TPAMI.2018.2818162, 22 March 2018

[5] Muzhir Shaban Al-Ani ; Tishko N. Muhamad ; Hersh A. Muhamad ; Ayub A. Nuri , "Effective fingerprint recognition approach based on double fingerprint thumb",ICCIT, 03 July 2017

[6] Sheng LiDong., "Pattern Recognition. Beijing", Beijing university of posts and telecommunications press. 2010.

[7] Mouad. M.H. Ali; Vivek H. Mahale ; Pravin Yannawar ; A.T. Gaikwad, "Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching",Advance Computing Conference, IACC, IEEE International, 2016

[8] Cao Weiguo; Wei Jinyu, "USB disk based on fingerprint encryption and supporting password generation and USB disk encryption method", google patent, 2017

[9] Cooley Robert [GB]; Baranowski Roland [GB]; Howell Christopher [GB]: "Accessing remote data or programs via a shell application from a portable memory device running in a virtual machine on a pc", google patent, 2011

[10] Zhao Jianji, "USB key",google patent, 2018

[11] Mao Juyong; Li Peisheng, "A data storage device with the function of fingerprint identification and lock" ,google patent, 2018

[12] S. Ghosh, A. Rana, V. Kansal, "A Novel Model Based on Nonlinear Manifold Detection for Software Defect Prediction" in Proceedings of the 2nd International Conference on Intelligent Computing and Control Systems, ICICCS 2018, pp 140-145 (2019).

[13] S. Ghosh, A. Rana, V. Kansal, "Statistical assessment of nonlinear manifold detection-based software defect prediction techniques" in International Journal of Intelligent Systems Technologies and Applications, Vol. 18, Issue 6, pp579-605 (2019).

[14] H. Walia, A. Rana, V. Kansal, "Case based interpretation model for word sense disambiguation in Gurmukhi ", in Proceedings of the 9th International Conference On Cloud Computing, Data Science and Engineering, Confluence 2019, pp 359-364 (2019).

[15] How software size influence productivity and project durationInternational Journal of Electrical and Computer Engineering

[16] S. Ghosh, A. Rana, V. Kansal, "A statistical comparison for evaluating the effectiveness of linear and nonlinear manifold detection techniques for software defect prediction" in International Journal of Advanced Intelligence Paradigms, Vol. 12, pp 370-391 (2019).

[17] M. S. Meena, P. Singh, A. Rana, D. Mery, M. Prasad, "A Robust Face Recognition System for One Sample Problem", in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp 13-26 (2019).

[18] B. N .Pandey, A. K. Shrivastava, A. Rana, " A Literature Survey of Optimization Techniques for Satellite Image Segmentation", in International Conference on Advanced Computation and Telecommunication, ICACAT 2018 (2018).

[19] P. Navaney, G. Dubey, A. Rana, "SMS Spam Filtering Using Supervised Machine Learning Algorithms", in Proceedings of the 8th International Conference Confluence 2018 on Cloud Computing, Data Science and Engineering, Confluence 2018, pp 43-48 (2018).

[20] H. Walia, A. Rana, V. Kansal, "A Supervised Approach on Gurmukhi Word Sense Disambiguation Using K-NN Method" in Proceedings of the 8th International Conference Confluence 2018 on Cloud Computing, Data Science and Engineering, Confluence 2018, pp 743-746 (2018).

[21] S. Ghosh, A. Rana, V. Kansal, "A Hybrid Nonlinear Manifold Detection Approach for Software Defect Prediction" in 7th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2018, pp 453-459 (2018).

[22] H. Walia, A. Rana, V. Kansal, "Word Sense Disambiguation: Supervised Program Interpretation Methodology for Punjabi Language ", in 2018 7th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2018, pp 762-767 (2018).