

How to Cite:

Pardhi, P. R., Borikar, D. A., Pardhi, M., & Shukla, G. (2022). Device-based password management system (bulwark). *International Journal of Health Sciences*, 6(S1), 10484–10494.
<https://doi.org/10.53730/ijhs.v6nS1.7531>

Device-based password management system (bulwark)

Praful R. Pardhi

Shri Ramdeobaba Collge of Engineering and Management, Nagpur, Maharashtra, India

Corresponding author email: pardhipr@rknec.edu

Dilipkumar A. Borikar

Shri Ramdeobaba Collge of Engineering and Management, Nagpur, Maharashtra, India

Manish Pardhi

Shri Ramdeobaba Collge of Engineering and Management, Nagpur, Maharashtra, India

Gaurav Shukla

Cognizant System, Pune, Maharashtra, India.

Abstract---Password manager systems currently available for the users come with serious privacy and vulnerability issues of their own. This paper gives an introduction to Bulwark, a novel device-based password management system, which stores the login credentials on a mobile device, and can enter the credentials on any target device through an encrypted cross-platform system, only after being authenticated by the user biometrics to ensure that only the right user can fill the saved passwords. This technology aims to eliminate the need to trust and rely on third-party cloud-based services or computers with storing and managing our passwords, and has also resolved major privacy and vulnerability issues with the current options available for users.

Keywords---Encryption, Cyber Security, Password Management, Fingerprint Authentication, Browser Extension, Socket Programming, Java Server Program, QR Code.

Introduction

The more the world is moving towards digitalization, more and more security concerns are being raised every day. It is true to say that, “Credentials are

peoples' new Identity", and no one wants their identity to be compromised. Online threats are increasing day by day and credentials are being compromised every hour. Broadly, online attacks are classified into different types, be it shoulder/CCTV surfing, DDOS attack, brute-force, phishing, and many more such ways. The need of the hour is to get a solution that is so robust that could let users be free from all of these attacks and credentials should never be compromised again. The main purpose of our research paper is to build an end-to-end encrypted solution equipped with the latest security standards also making the user's life easier [7].

We came up with our solution, Bulwark, an on-device-based password management Android-application. Next time, while you are browsing a website on a PC/Laptop and it asks for your credentials, you just need to put your Fingerprint on your local phone and your credentials will automatically be provided to the-Website. You might be concerned about exactly where your credentials will be stored. Your credentials are safe in your local phone encrypted with the latest AES256 security standards providing you top-notch security against Brute force attacks [6].

While we were developing a solution, we thought of Pin/Password authentication, but passwords/pin can be compromised through shoulder/CCTV/drone surfing attacks, we then implemented Biometrics in our solution providing you yet another relief of not remembering-PIN/Password. The system we designed consists of a Phone, a Laptop, and a necessary condition to make sure is both of them are connected on the same network giving you another relief through DDOS attacks. You just need to scan the QR code and make sure the Laptop and mobile are connected so that you can enjoy our solution.

Methodology

We designed the application that manages the storage and retrieval of passwords for different website accounts and the application. We used SQLite database for the storage of users' credentials which are located in personal mobile devices. The passwords can be viewed or filled in only through fingerprint authentication. The architecture of the system is consisting of three main components, i.e. the Android Application, Browser Extension, and Native Java Server Program.

Fig. 1 shows the architecture of the password management system and the interaction between the three main components. The Browser Extension starts the Native Java Server Program, the server program in turn gets the local IP address of the PC and generates a QR Code for the same. Meanwhile when the application starts, it authorizes the user, connects using IP or QR Code, and accepts the server requests on a separate thread. The browser then sends the website URL opened in the PC to the server which sends it to the application. The application searches the URL in its SQLite Database and if the entry exists, it first authorizes the user again via fingerprint and after authentication sends the credentials to the server in encrypted form using the AES-256 encryption technology. The Extension then gets the credentials from the server and fills them in the provided input space on the webpage.

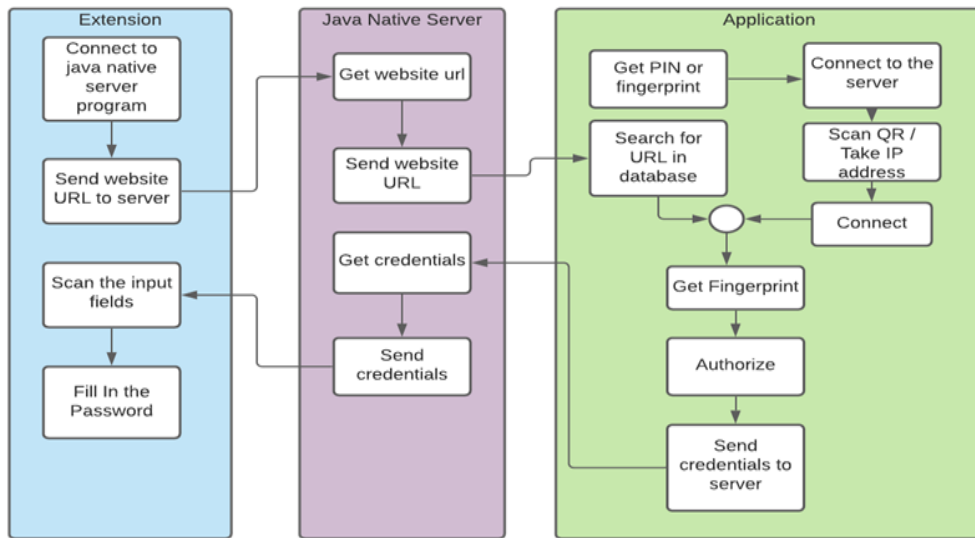


Fig. 1 Architecture of Password Management System

Implementation

We developed an android application with different application components to control and manage the different functionalities of the system. We also used java socket programming for intercommunication of android to windows software. The working of the three main components of the system is shown by the flow diagram in Fig. 2, Fig. 3 and Fig 4 [4]. In the QR Code Scanning module – a QR code scanner is implemented to scan QR codes generated by the native server program.

Advanced Encryption Standard (AES)

AES-256 is used in the application for encryption purposes. AES is the most secure encryption standard available. AES-256 is the strongest encryption standard with a key length of 256 bits which is the greatest bit-size. Due to this, it cannot be practically broken using brute force as far as the current computing capability is concerned. AES uses only one secret key to both encrypt and decrypt the data which is called symmetric key encryption. In the proposed work AES is implemented in the android application for password encryption, this encryption method is implemented as an activity in the android application. AES-(256) encryption algorithm is used for the implementation [1], [5].

Browser Extension

Browser extension is implemented via HTML, JavaScript, Json, PNG, and Icon files. Java socket programming is used for the communication of browser extensions with the native Java server program [2].

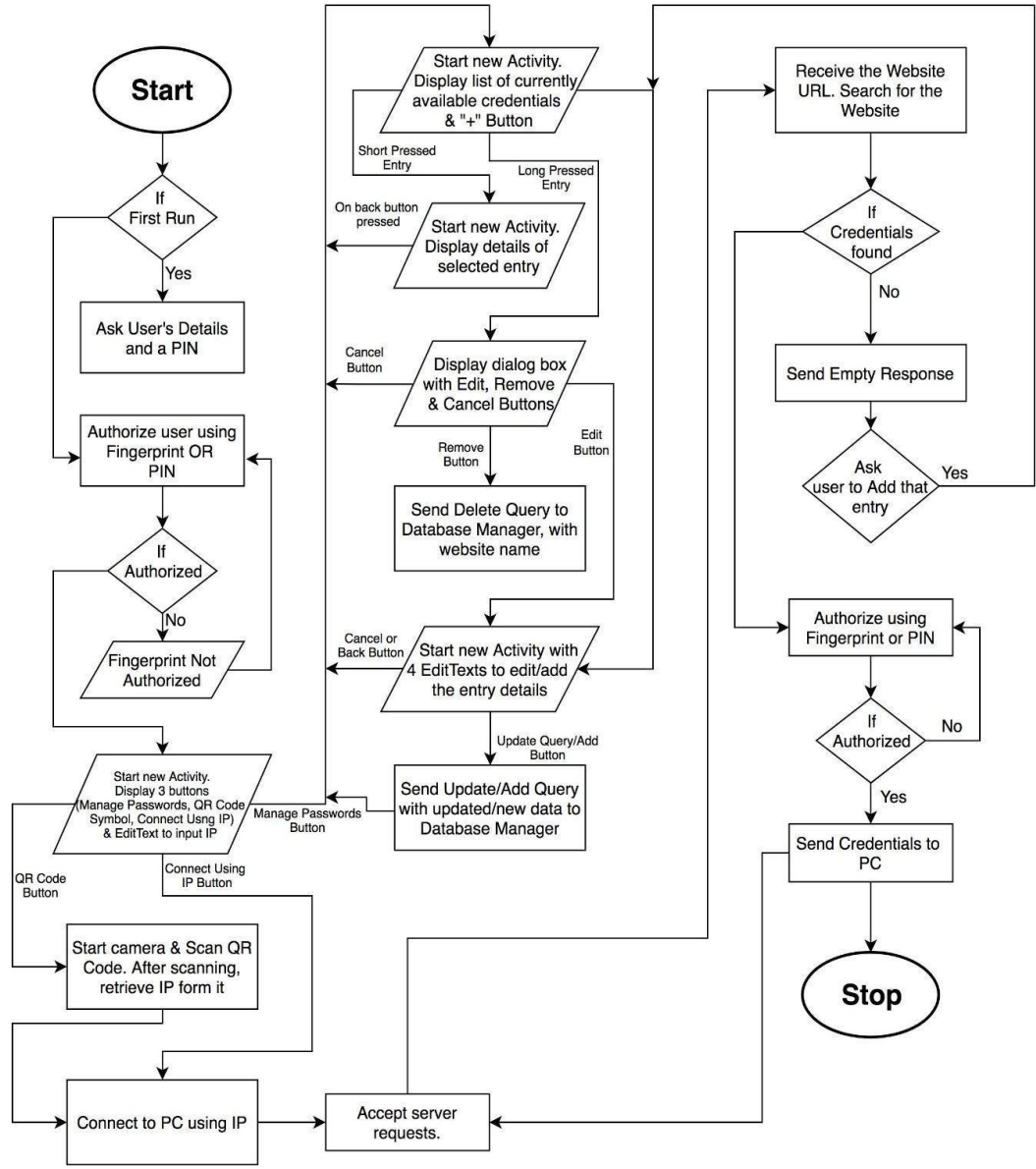


Fig. 2 Flow of Android Application

Native Java Server Program

This software is purely implemented using java, in this application; a QR code generator is implemented to establish a connection between the android app and this Native Server Program. This program helps in establishing a connection between the PC and mobile phone, to enable the browser extension and android app to interact with each other for information transfer [3].

Fingerprint Authentication

Google's fingerprint API for android has been used to implement the fingerprint authentication part.

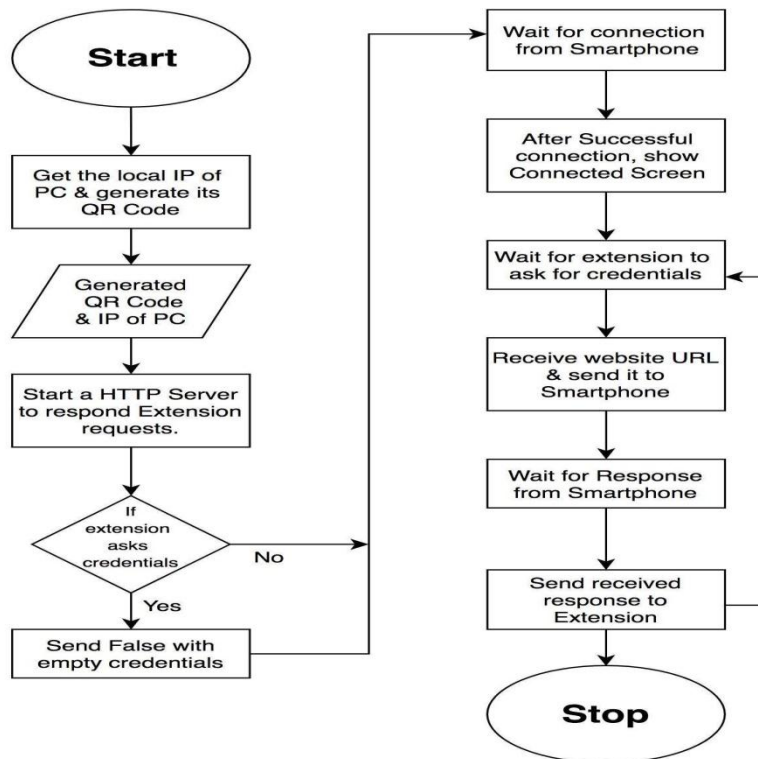


Fig. 3 Flow of Native Java Server Program

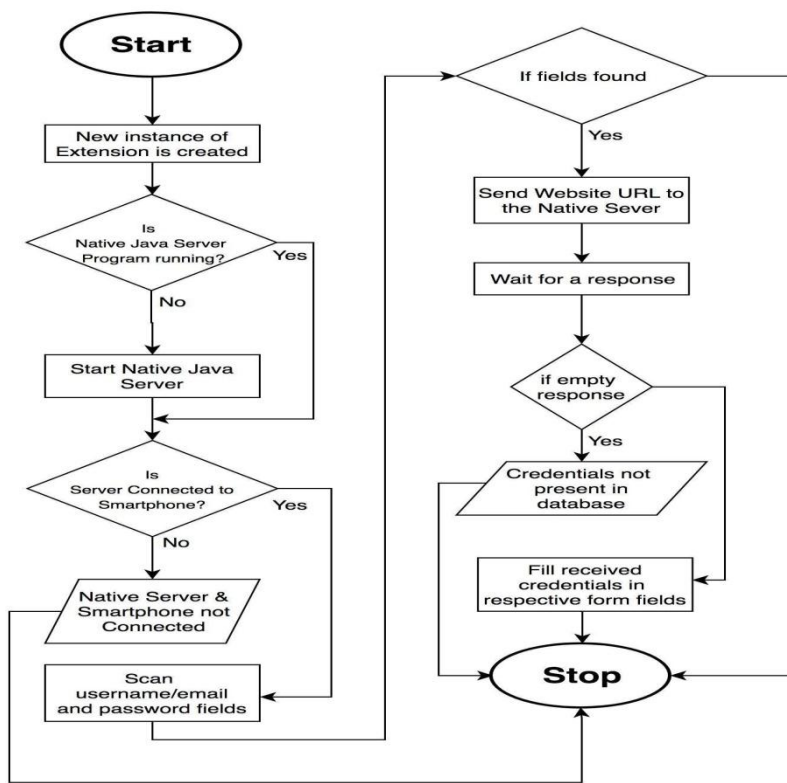


Fig. 4 Flow of Browser Extension

Results

We implemented the proposed system that works successfully on mobile phones. Screenshots in Fig. 5 through Fig. 11 show the working of the system in detail. The app provides automated login to the web page that the user intends to work on without typing in the password, username, or email id. In this application, all the permissions lie with the user, i.e., they can add the web page details in their device so that they could log in with a touch of a finger on the fingerprint scanner of their mobile phones, they can delete the data if not further needed from the database of the phones and can even edit the password if they have changed it.

Main Screen

Fig. 5 shows the main screen of the android application. This is where the user is authenticated using a fingerprint. If not, the user clicks the “VERIFY USING PIN” button.

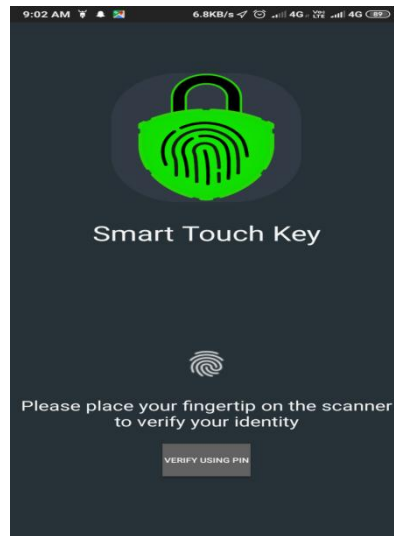


Fig. 5 Main Screen of the application

Verify using PIN Screen

When the user clicks the “VERIFY USING PIN”, this is the pop-up which appears in Fig. 6 which takes the PIN as input and has the “OK” option which when clicked, the user moves to the connecting screen, the other option “CANCEL” leads back to the main screen.

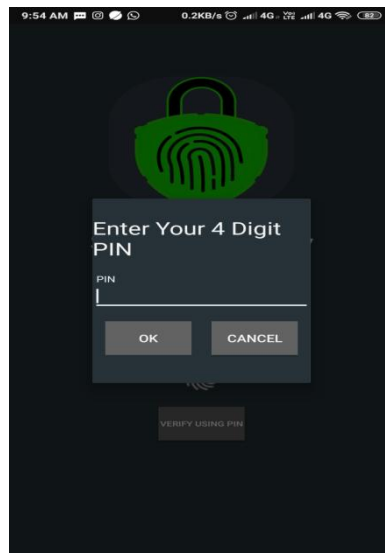


Fig. 6 Verify using PIN Screen

Connecting Screen

Fig. 7 allows the user to proceed by scanning the QR code to connect the mobile phone with the user's PC. Here either one can scan the QR code generated on the

PC or can manually write the IP address of the PC. There is a button named “MANAGE PASSWORD” where one can manage the data.

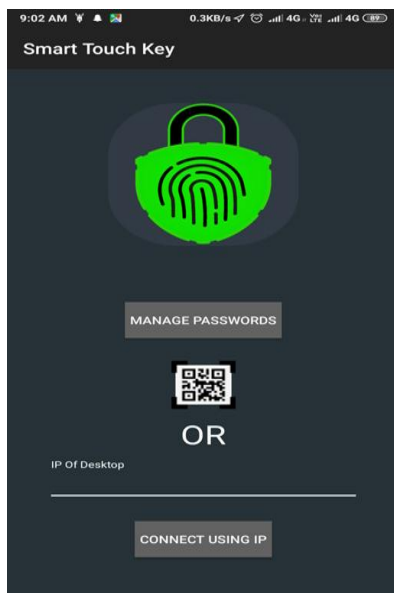


Fig. 7 Connecting Screen

Manage Password Screen

In Fig. 8 the user can manage the data regarding web pages and their passwords. A button with the sign “+” located at the right corner is used to add a new entry.

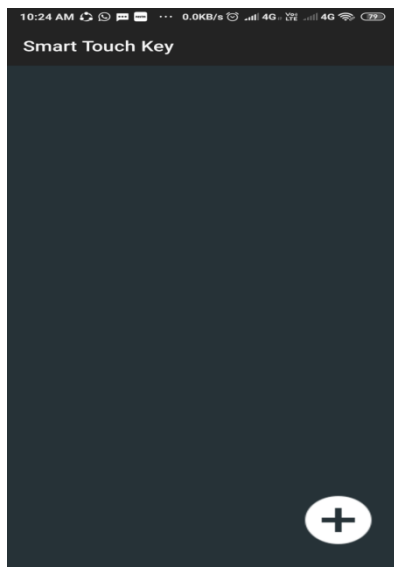
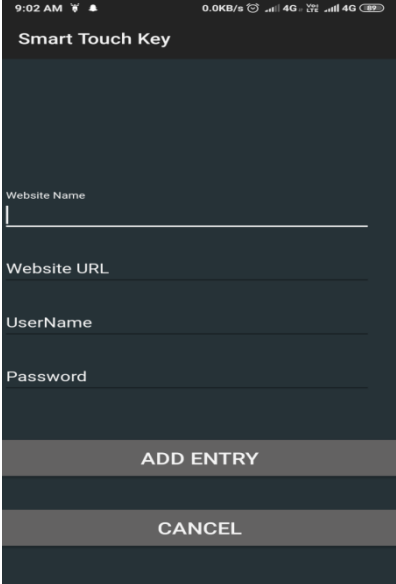


Fig. 8 Manage Password Screen

Extended Screen

In Fig. 9 on clicking the plus button in the manage password screen, this button helps the user to add the details manually. The page contains four text fields i.e., “WEBSITE NAME”, “WEBSITE URL”, “USER NAME”, and “PASSWORD”. The password is stored in the database in encrypted form. There are two buttons namely “ADD ENTRY” which adds the new entry to the database and the “CANCEL” button which cancels the entry.



The screenshot shows a mobile application interface titled "Smart Touch Key". At the top, there is a status bar with the time "9:02 AM", signal strength, and battery level. Below the title, there are four text input fields labeled "Website Name", "Website URL", "UserName", and "Password". At the bottom of the screen, there are two buttons: "ADD ENTRY" and "CANCEL".

Fig. 9 Extended Screen

PC Connection Screen

A connection is made between the mobile phone and the PC. The software (native java server) generates a QR code that contains the IP address of the PC. By scanning, this code connection can be established. Fig. 10 also contains a button “RESTART”, if there is any problem, clicking this button would restart the software.

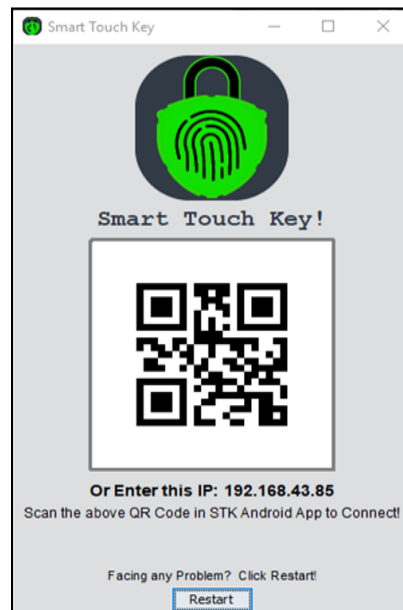


Fig. 10 PC Connection Screen

Fig. 11 appears on successful connection establishment.

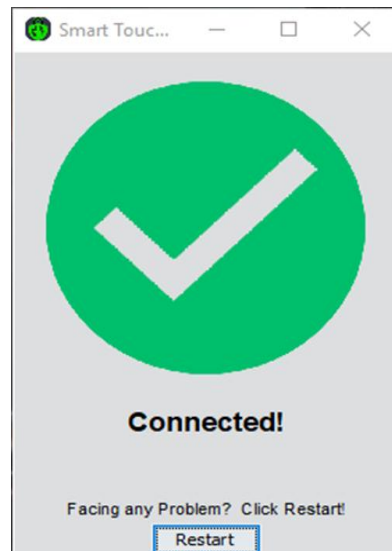


Fig. 11 Connection Established Screen

Conclusion

In this paper we have discussed how the device-based password management system technology works and how it has resolved all the major issues with options available for users currently. With increasing information literacy and increasing mistrust in cloud-based services, BULWARK's device-based architecture is the best option for the users since it enables the users to have

maximum control over their passwords and private information. A user-friendly interface, ease of access due to QR codes, and portability due to cross-platform architecture, makes Bulwark a game-changer. With practical utility and state-of-the-art technology, this technology will soon bring a disruption in the entire password and information management space globally.

References

1. AkoMuhamad Abdullah, Advanced Encryption Standard (AES): Algorithm to Encrypt and Decrypt Data, Cryptography and Network Security 2017.
2. Erdem E, O. Kucukkurt K., Samurkas, E. Kanargi, and U. Celikkan, A smartcard-based Single Sign-On and password management solution as a browser extension, International Conference on Education and Management Technology 2010, pp. 539-543.
3. Dhawan M and Ganapathy V, Analyzing Information Flow in JavaScript-Based Browser Extensions, Annual Computer Security Applications Conference 2009, pp.382-391, DOI: 10.1109/ACSAC.2009.43.
4. Yildirim N and Varol A., Android-based mobile application development for web login authentication using fingerprint recognition feature, 23rd Signal Processing and Communications Applications Conference (SIU), 2015, pp. 2662-2665, DOI: 10.1109/SIU.2015.7130436.
5. ShripalRawal, "Advanced Encryption Standard (AES) and It's Working," International Research Journal of Engineering and Technology (IRJET) 2016.
6. Dee T., Richardson I., Continuous Transparent Mobile Device Touchscreen Soft Keyboard Biometric Authentication, 32nd International Conference on VLSI Design and 18th International Conference on Embedded Systems (VLSID) 2019, pp. 539-540, DOI: 10.1109/VLSID.2019.00125.
7. KhedrWalid, Improved keylogging and shoulder-surfing resistant visual two-factor authentication protocol, Journal of Information Security and Applications 2018, Volume 39, Pages 41-57.