Multi-Layered Electronic Security System for Vaults

G.M.C.M. Bandara, A.T.R. Athuraliya, Ama Bandara, Udesh Oruthota *

School of Engineering, Sri Lanka Technological Campus (SLTC Research University), Padukka 10500, Sri Lanka

*udesho@sltc.ac.lk

Abstract - Vaults in the banks are mainly used to store valuable assets; for instance, cash, jewelry and documents, where they provide adequate protection from theft, fire, cataclysmic events, and other possibilities which can cause damages. In considering security systems for vaults, mechanical keys and the vault's exterior play a major role even though they are unable to guarantee an effective protection and the limited number of security layers has made it easy for burglars to break in. Henceforth, we have proposed to develop a multi-layer security system for vaults which mainly focuses on keeping the unauthorized people and/or thieves away from the rightful user's belongings. This paper discusses a system that consists of three independent layers where it includes fingerprint scanning, radio frequency authentication, face recognition through a software application included with a random code generator. The proposed system will be a smart reliable secure solution in compared with existing designs and an initial model will be implemented to validate the outputs.

Keywords: Authentication, face recognition, random code generator, Radio frequency identification, Security System, software application

I. INTRODUCTION

Current security systems consist of various technologies which are built around the vault`s locks and has more of a traditional approach. Basically, it has one or two locks; a combination lock and/or a two key lock which is completely independent from one another. Some locks consist of a digital keypad where the user has to enter the password manually. The system inside varies from vault to vault. As of present, types of vaults/safes used by banks in Sri Lanka are BS 108, BS-125, executive safe with digital lock, defender, deluxe safe etc. Apart from the lock, one of the techniques used in vaults is the tool and torch resistances which are also known as burglar resistance where the protection from a torch and tool attacks are secured [1]. Some vaults are made to be fire resistant for about 1-2hours, in which the vault's safety is guaranteed in the event of fire or even water, anti-hold up resistance alarms when the safe is being removed from its original location. Fort Knox in United States [2] has an outstanding security system which includes a granite wall perimeter, squadrons of machine-gun wielding guards, armed military and a 22-ton vault door and it requires minimum of 10 people just to open the vault. In the New York federal reserve vault [3], pallets are moved around by robots.

The bank of England gold vault [4] is quite popular for having bombproof walls, a voice recognizing system which has 3-foot keys and other unknown security techniques. In 1914, The Dominion Bank Vault was renowned as the most secure bank vault in the world for its construction and the 40-ton vault door. These vaults are considered as safe, reliable and hard to break- in but one of the main drawbacks of these are that they focus on the exterior mainly. In most situations, anyone who has the key/keys will be able to open the vault even though the vault does not belong to them. It is hard to keep track of the vault's key/keys and even if the vault has a digital keypad, one must ought to remember the passcode. By any chance if you misplaced the key/keys or forgot the passcode, you won't be able to open your vault, at least not in that exact moment. Thus, key-based systems can have multiple safety concerns.

In general, people have limited access to bank vaults considering the fact that they are allowed to enter their bank's vault only when the bank is open, proving why the private safes/ vaults are getting more popular. Apart from the traditional approach and giving priority to the exterior, various systems have been proposed which does not require a lot of manpower and will be secured by a 3G Wi-Fi dongle, cameras and bio-metrics. Some are proposed to consist of several types of sensors including, gas, ultrasonic, laser, motion sensing etc. Even though it is admirable that people tend to seek for more modernized, software-based systems which focuses on authentication more, there are still areas to pay attention to and secure. Henceforth, as a smart solution we propose a four-layered, safer, more modernized and smart security system which can protect the vault from unauthorized people and/or theft. This system is a combination of a biometric system and an access control system where we expect to create a software platform with a random code generator to create specific codes for the authorized person as an input password to the system. The random codes will be validated twice through the software before entering to the system with a unique changing sequence.

II. MATERIALS AND METHODS

A. *Hardware subsystem:*

Fingerprint scanner: A fingerprint scanner is used as the first authentication layer for the bank vault system which consists of a universal asynchronous receiver-transmitter (UART) interface, hence it has to be interfaced with Raspberry Pi through a universal serial bus (USB) to serial converter module.
Radio Frequency Identification (RFID) system: An RFID tag is used as an authentication tool in which the system checks whether it is authenticated or not when the user places the RFID tag on the reader module.

Image capture system: A Pi Camera is used in the proposed vault system to capture an image of an intruder who tries to

access the vault. The captured image will be sent to a designated user as an email attachment.

Human machine interface: A liquid-crystal display (LCD) display is used to display instructions on entering the one time password (OTP) codes required to open the bank vault whilst an alphanumeric keypad was selected to enter the OTP codes required to open a bank vault.
Alarm system: An alarm is raised when the system detects unauthorized attempt to access the vault.

B. *Software subsystem:*
Random code generation algorithms: Two randomly generated OTP codes are created in two instances to open the bank vault, where the second codes map with a unique sequence.
Image capture and emailing: A photo of an unauthorized person is captured by a pi camera module is emailed to an authorized person using Wi-Fi.

Android application: This Android app is used to determine if the entered randomly generated code matches with the code that has been sent to the user's mobile. It also creates another randomly generated code by mapping the first code into an algorithm. This application will not be available to download from the play store; the user can install the application after making a request from the creator.

The flow chart of the proposed design is illustrated in Fig. 1. Prior to the vault security system, an RFID based identity card authentication is carried out to reach the vault by the user. Once the access to the system is provided, first a fingerprint scanner module and face recognition system are used parallelly to check if the person is authorized. This scanner module and the detection system are connected to the front surface of the vault. After the authentication, the user will have to enter the first pin code which will be generated randomly by the vault's system computer, which is sent to the user's mobile phone through a cloud data base. Internet connection to the vault's computer is established through a 3G modem/dongle. The user has to view the received OTP from their phone and enter this code into a software application which will be available for the authorized users only. Once the OTP is verified by the application, it moves to the third layer of security.

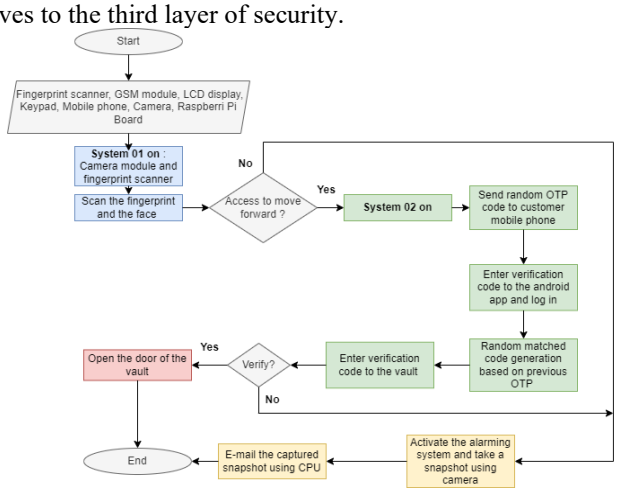

Fig. 1 Flow chart of the proposed design

The application will display another randomly generated code which is created by mapping the first generated code to another algorithm (Ex: 6789) in the app. So, the person will have to enter this code (6789) as the second pin code when it is requested by the vault. The verification will be done through a centralized cloud server, where the data is updated sequentially based on the user id and the application random code generation. After successfully completing all the above processes, the vault will be unlocked. In each step, if an unauthorized person attempts to open the vault and fails to verify themselves, a camera is installed on the vault to capture a photo of the suspect and send it as an email to an assigned authority. Simultaneously an alarm will also be raised. Here, a battery backup will be kept alongside rather than the power supply because it will increase the safety during a power failure or any other breakdown situation. For this purpose, a battery with a charging unit will be used.

III. Results And Discussion

In the Android app, the registration page in order to create an account, the login page which allows the user to login using a username and a strong password and a page to enter the first random generated OTP have been created thus far. The procedure to save this entered OTP in the Google Firebase has also been completed. Generating the OTP and sending it to the user's mobile phone through short message service (SMS) gateway and creating the image recognition algorithm will also be focused on. This process will let the user to verify themselves through the OTP and their facial features. In the fingerprint layer, the user will have to place their finger to get verified where an alarm system will go off in the event where an unauthorized person tries to break in to the vault. If the person who tries to open the vault is the rightful owner of the vault, they will be able to go to the vault once they verify themselves successfully in all these layers.

The proposed system has few limitations such as if the system is designed to be powered by an AC to DC adapter with no battery backup, a standalone power supply unit is mandatory since the system can become vulnerable to unauthorized access during a power failure. Even a legitimate user with proper access, will be barred from access to the vault contents during a power failure. Designing an adequate battery backup is a process that consumes some additional time and resources, which is proposed as a future development.

IV. CONCLUSION

This paper discusses on an authentication-based electronic security system which has the ability to provide protection to one's possessions while reducing break-ins where the vault's safety is ensured by creating a burglar deterrent environment. The system also provides protection to the user as well, since they will be prevented from confronting a burglar. This concept will be implemented further by granting access through voice recognition and in the event of power failure. Adequately encrypted data transferring and introducing a proper cooling mechanism are to be included in the future development while

creating future paths to raise awareness on upcoming and developing security-related technology features.

References

[1] R.Kolins. Safes, vaults, and accessories. Handbook of Loss Prevention and Crime Prevention, Pp 433–443,.2020

[2] P.Holtewert, R.Wutzke,J. Seidelmann, & T.Bauernhansl. Virtual Fort Knox Federative, Secure and Cloud-based Platform for Manufacturing. Procedia CIRP, 7, Pp 527–532,2013.

[3] Germany's gold at the New York Fed: is it still there? (n.d.). Retrieved July 15, 2022

[4] S.Manning. The Bank of England as a bank. Bank of England Quarterly Bulletin, Vol.54, Pp 129–136,2014.