Server-specific add-on biometric security layer model to enhance the usage of biometrics

Bhanu Singh ^{1,*}, Nirvisha Singh ²

¹ Information Technology and Services, Perrigo Plc., Michigan-49011, USA; bhanu.singh@perrigo.com

² Department of Neuroscience, Central Michigan University, Mt. Pleasant, USA; singh3n@cmich.edu

* Correspondence: spbhanu201@gmail.com

Received: date; Accepted: date; Published: date

Abstract: With high paced growth in biometrics, and its easy availability to capture various biometric features, it is emerging as one of the most valuable technologies for multifactor authentication to verify a user's identity, for data security. Organizations encourage their members to use biometrics, but they are hesitant to use due to perceived security risks. Because of its low usage rate, many medium and small segment organizations find it unfeasible to deploy robust biometric systems. We propose a "server-specific add-on biometric security layer model," to enhance confidence in the usage of biometrics. We tested this model via a biometric mobile app, and the survey showed a favorable response of 80%. The innovative mobile app was tested for its usability and got a score of more than 71%. For test tool reliability, we examined the equal error rate (EER) of the app and got a reasonably low score of 6%. The results show a good potential of this framework to enhance users' confidence-level in the usage of biometrics. Higher usage rates may make deployment of biometrics more cost-effective for many organizations to decrease their information security risk.

Keywords: Biometrics; mobile applications; data security; privacy; cyber security.

1. Introduction/ Background

With high paced growth in biometric technology (a.k.a. biometrics), it has become a focus area for many future investments [1]. Large companies are deploying resources in many industrial and consumer applications such as EEG controlled 3D maze, fingerprint identification kits, park passes, smart home, and industrial devices. [2]. Large healthcare organizations like Sentara Healthcare, Norfolk, have invested in "biometric palm vein identity authentication" for their patients to access their health records, remotely [3]. As per reports from Statistics MRC, "the Global Identity & Access Management Market is expected to reach \$20.87 billion by 2022, with a growth rate CAGR of 14.8%" [4]. The biometrics market for global healthcare is estimated to reach \$11.7 billion by 2024 [5].

Many modern solutions such as door-locks with fingerprint, laptops, tablets, smartphones, firearms-locks, customer voice response (CVR) systems with voice identification, smart-doors, smartphones with face recognition, etc. have been trying to adopt biometric identification with varying degrees of success. One of the reasons for fast growth in biometrics is that, like many other applications, it is slowly emerging as a service, "BaaS" (biometric applications as service) [6].

With the fast growth of biometrics, as BaaS, in the cyber world, especially for the usage with IoT devices, there comes security vulnerabilities. Most of the IoT devices and services such as modem,

41 routers, virtual assistants, collect and store information from other equipment and applications for
42 full utilization of their functionalities. Still, this interdependence makes all the devices vulnerable to
43 internal and external attacks [7]. In the heterogeneous IoT ecosystem, one powerful computational
44 device communicates with another powerful computational device, many times via some low-end
45 and not-so-secure devices. These less secure weak links put up a significant challenge to implement
46 robust security mechanisms [8].

47
48 The IoT ecosystem (devices and services), is still not entirely trustworthy because they face
49 many challenges due to the characteristics of cyberspace where threats from organized intelligence
50 and criminal groups are more challenging to defeat than from individual hackers [9]. Therefore,
51 the fast growth of biometrics in cyber-society without some extra layers of security may pose some
52 big problems, especially for medium and small healthcare organizations. The reason small and
53 medium healthcare organizations are more vulnerable is because their customers and patients are
54 more focused on their health issues than systems' security. Moreover, unlike banks and financial
55 organizations, healthcare organizations lack fraud detection and security teams. Hackers may steal
56 patient medical records, clinical trial data, and drug development-related information, which may
57 increase counterfeit drug trafficking and medical insurance fraud.

58
59 The above studies indicate that our personal and corporate data are at a higher risk than ever
60 before. So much so that organizations and private people are slowly trying to learn to protect their
61 data with a mix of biometric technologies [10].

62
63 Large corporations, especially large banks, have been encouraging their customers to
64 download their app and use biometric data such as fingerprints for multifactor authentication (MFA).
65 The biometric-based m-banking (mobile banking) applications used by large financial institutions are
66 complex and costly to deploy. They have colossal fraud detection and prevention teams to detect
67 fraudulently run operations via IoT devices. Users also are covered through insurance if such
68 fraudulent transactions are quickly reported to banks. Users can download the banking app from the
69 bank's website after logging in and install on any of their mobile devices. They can use either login
70 and password or use the sensor for fingerprint or facial recognition, depending on the model of their
71 mobile device.

72
73 These apps are allowed to be installed on any device. Users can get SMS and or email alert if
74 they have agreed to and saved this in their user profile. However, some security concerns have been
75 raised by many critics against the mass usage of such apps. Many users do not choose the notification
76 option in their user profile to avoid too many alert messages. A large percentage of users use obvious
77 user-id and password. A hacker can install the banking app on any device, steal user-id, password,
78 enter the DOB or pet's name, and perform fraudulent transactions without the user knowing about
79 it for a long time.

80
81 Even if a user has saved notification option in their user profile and chosen to use fingerprint-
82 based login, a hacker can spoof a user's fingerprint and perform fraudulent transactions. Only very

vigilant type users may be able to take immediate corrective action with the help of the technical support team of the bank. Researchers have proved that fingerprints spoofing are not very difficult. There have been cases of fingerprints being spoofed [11]. There is a higher possibility of fingerprint spoofing in a hospital environment, despite the data and privacy protection rules such as the Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), etc. [12].

General Data Protection Regulation (GDPR) has standards for protecting the patient's health records. But it would take a long time to detect such security breaches if this happens in the healthcare industry because hospitals usually do not have a dedicated fraud prevention team. It is much easier to steal someone's password, User-id (UID), and type in the date of birth (DOB) or pet's name on a keyboard than to spoof someone's fingerprint or any biometric information and use it effectively [13]. Therefore, large healthcare companies are encouraging their users to use biometric technologies for user authentication via m-Health (mobile health app). But because of the low usage rate, many small and medium healthcare companies are not finding it very cost-effective to deploy a very robust MFA application system. A large percentage of users refrain from online usage of biometrics for privacy, security, and data leak issues. We propose a "*server-specific add-on biometric security layer model (SSABSLM)*," to enhance the confidence in the usage of biometrics. This model is based on the premise that certain applications are more critical to users, and building confidence in the access of those applications is more important than providing a general level of extra security layer to many applications. To test SSABSLM, we designed, developed, and tested a low-cost mobile app "Bio-Guard," to provide an extra layer of biometric security for the access of a web-based application via mobile devices. Then we surveyed a reasonably large sample population for the success of this framework. The mobile app solution framework is described in sections 3 (technology) and 4 (experiments). We have presented experimental outcomes, survey results, and analysis in section 5. Section 6 presents implementation opportunities and challenges. Section 7 concludes with some future perspectives. In the next section 2, we discuss some of the relevant authentication modalities, types of communications used for authentication, and the related factors which can impact these processes.

2. Related Works

The IoT ecosystem is open or semi-open to many types of users, including hackers and adversaries [14]. To improve security in the entire IoT chain, the focus of research work is shifting towards more robust user authentication. The goal of authentication is to verify the legitimacy of the person or device who is trying to access a system. There are many ways and means to verify a user's identity. One of the most often mentioned classification schemes of authentication is based on something-you-know (SYK), i.e., password, something-you-have (SYH), i.e., smart-card, and something-you-are (SYA), i.e., biometric features such as retina-print, as discussed by [15], [16]. Ferrag *et al.* [17] presented authentication schemes of mobile devices into four categories **a)** factor-based, e.g., 2-Factor, multi-factor, **b)** channel-based, i.e., Seamless roaming [18] **c)** ID-based, i.e., remote user's authentication [19] and **d)** biometric-based.

As per Traore *et al.* [20], authentication can be divided into two categories: *static and continuous*. The static user authentication gets invoked one time at the beginning of a communication session, e.g., to verify the user's password/ PIN [21] or facial-features [22]. The continuous authentication gets repeatedly invoked to verify the legitimacy of a user based on touch or mouse

movement/ click or keystroke during the time of device usage [23]. Unfortunately, most of the smartphone authentication methods follow the static authentication process, which cannot provide seamless certification. Therefore, static authentication becomes prey to session hijacking attacks. To overcome the issue of static authentication of biometric features and cryptographic methods, Robertas *et al.* [24] proposed EEG based biometric cryptosystem. This biometric cryptosystem has low explosibility and can be used by disabled people or users with some missing physical traits. For Continuous authentication, Guannan *et al.* [25] suggested a two-step authentication method based on motion and physiological movement, i.e., photoplethysmography (PPG) signals, especially for wearable devices. Even continuous authentication protocols can be classified into two categories: *a) user-to-device and b) device-to-device* [26].

Based on the review of the above literature, it appears that the continuous authentication method mixed with biometric features and physiological movement can address many security issues of mobile devices and applications [27]. However, each of the biometric characteristics such as fingerprints, iris, electroencephalography (EEG) data, voice, face, palm, ear, and gait, has its advantage or disadvantage. For example, age has minimal impact on features of the ear, and it can be a very convenient source of data for *passive biometrics*, but continuous authentication of the ear is difficult [28], [29]. Robertas *et al.* [30] discussed gait (a person's walking pattern) based biometric feature which can be, unobtrusive, implicit, and passively observed continuously, so long as the user is carrying her/ his smartphone or is around it, though gait can be affected by many factors such as shoes, stimulants, mood, aging, etc.

The “*hardware-based biometric security access technology*” of prominent vendors like HP and Microsoft are primarily designed for mass usage. There are many sensitive software applications mainly related to patient health records, which would need more specific protection. To provide a different level of eHealth record access to different the personnel of varying rank Spanakis *et al.*, proposed SpeechXRays, a multi-channel biometrics platform of user authentication [31], [32]. This framework is based on a multi-modal authentication paradigm [33] based on voice acoustics facial recognition [34]. The fundamentals of this approach are excellent; however, devices to collect relevant data and willingness of users to share all those data at the moment could be a challenge.

Recently mobile devices have started focusing on 3-D orientation of the biometric sensors. It has led to many research works in touch and “*gesture-based*” continuous authentication, even though there are variations in the captured touch data, depending on the user's posture, despite the similarity in the device specifications [35]. These continuous authentication techniques have inspired us to develop something novel, flexible and scalable, and we developed a mobile app framework, “Bio-Guard.” This app framework uses a continuous authentication method based on session-id, which is in line with the latest schemes of light-weight authentication technique recommended to be used in the era of IoT, IoS (Internet of Sensors) [36]. The adaptability of the Bio-Guard app distinguishes it from many other mobile app frameworks because it can adapt to any cryptographic or biometric features, used by the users via their mobile device. The architecture of the Bio-Guard app is open to be aligned with multi-modal authentication and NGI systems.

2.1. The Rationale behind the usage of the Bio-Guard App, as an “add-on” to Test the SSABSLM

There are apps deployed by large financial institutions that can send a notification to registered users if someone logs in to users' accounts from another device and performs some activities. There are *hardware-based fingerprint readers* like that of "Windows Hello" and HP's USB fingerprint reader, that let a user verify a Microsoft account or a non-Microsoft service that supports Fast Identity Online (FIDO). Then why we needed an "add-on" app for an extra layer of biometric security to test SSABSLM?

2.1.1. There are many reasons to develop the Bio-Guard app, some of which are mentioned below:

- We did not find a feasible software solution that could fit in our model on the server-side and mobile device side to test the SSABSLM.
- Architecturally it is different in that it is a software-based and not a hardware-based extra layer of security.
- There is an extra cost associated with hardware replacement/ upgrade. A hardware-based extra layer of security may fail if there are any wear and tear related issues.
- Software-based security would be more scalable and flexible to adjust to the fast-changing security dynamics.
- This app will send "server-id" only to the verified users to complete the installation of the app without that users will not be able to access a particular application. In that, it is very targeted and server-specific and not a generic security layer.
- Most of the methods of the user or device authentication emphasize on one or a few aspects of the cryptographic or biometric features. Multimodal biometric systems combine many biometric features to make the authentication more scalable [37], and this app is architected on multi-modal lines. It can be used for any of the biometric features captured by smartphones.

2.2. *Scope of the App for Testing the SSABSLM*

Though the sources of research and examples cited in this paper are from many countries, the experiment and implementation aspect of the app is primarily scoped from the perspective of health care service providers of those countries where necessary infrastructure, rules, and procedures are in place, to start with.

3. Technology and Methods

This section presents *six subsections* to provide a broad overview of the "Bio-Guard" app framework: 3.1. Authentication process; 3.2. The Architecture and data flow; 3.3. System's requirements; 3.4. Installation process; 3.5. Error handling; 3.6. Current limitations of the app.

3.1. *Authentication process*

The web-based application to be accessed via the app user had Oracle11g as a database. Therefore, the secure hashing algorithm 1 (SHA-1) was used for biometric authentication because certificates signed via message digest 5 (MD5) algorithm face difficulty in HTTP /web environment [38]. A prototype application was developed using a 2-Tier architecture model. Oracle11g was used as a backend database that supports web-based biometrics authentication via oracle adaptive access manager (OAAM) [39]. For experiments mentioned in this paper, biometric characteristics from specific users were previously captured, and the model templates were stored in the database. The

fingerprint sensor of the user's mobile devices was used only for training and getting aligned with the existing template models. Minutiae-based fingerprint features were used during the test for user authentication because those templates were available in the application database of the web-application used for the testing to authenticate the testers [40]. For criminal investigation and record access, more advanced "next-generation identification NGI" systems are suggested by many researchers. For example, NGI systems may authenticate many aspects of biometric features such as tattoos, scars, etc. which can through light on gang membership, previous convictions [41]. However, for day-to-day access to applications, NGI systems may be too cumbersome for ordinary users.

For a better understanding of the authentication logic of the application, a summary of the variables and parameters to be verified are declared and explained in this subsection. The next section of data flow and validation describes how the variables will be compared and validated for access.

Ushered is associated with First + Last Name, DOB, Email, and Mobile device of the user, in the background web-application. UID verification in the background web-application is a separate process of that application. For example, if a company decides to use "employee id" or "patient id" or "company email" as UID, then that id must first exist before a user can register and receive OTP.

- User id $\rightarrow$ UID.
 - Server installation id (SID) $\rightarrow$ This is generated when the server-side of the app is installed.
 - Password $\rightarrow$ P.
 - OTP $\rightarrow$ O.
 - Client Installation id (CID) $\rightarrow$ This is generated when the client-side of the app is installed.
 - Biometric profile $\rightarrow$ B.
 - Registered Device id $\rightarrow$ RD(id) = IEMI number of a mobile device or Device id of a laptop + CID.
 - Combination of SID + CID + RD(id) $\rightarrow$ SCI(id).
 - SCI(id) = RD(id) + SID.
- SCI(id) comes only from those devices where the "Bio-Guard" app is completely installed.

3.2. Architecture, Data Flow, and Validation

3.2.1. When Bio-Guard app is not installed on the server, as shown in Figure 1, the system will grant web-access when the secret key stored in the security policy matches any of the following parameters:

- UID + P + O or
- UID + B

3.2.2. During the installation process of the "Bio-Guard" app, the system would require the SID to get associated with the security policy. Therefore, it would grant web-access when the secret key stored in the security policy matches any other following parameters:

- UID + B+SCI(id) or

- UID + P + O + SCI(id)

3.2.3. Once App is fully registered, and installation is completed, then a user needs only the following info to login to the FBAS:

- UID + P + O or
- UID + B

Figure 1. An architectural diagram is showing how Biometric authentication works via unmonitored OTP before installing Bio-Guard App on a Mobile device and Oracle Biometric Authentication server. The number 1a to 1d, and 2 to 5, show the sequential steps of data flow.

The mobile app is interfaced with a web app to push data to the central server. The app gets a GPS location from the place where it is connected to the internet. The functionality of the mobile app *Bio-Guard* is controlled by variables, based on Android studio code, an example of which is referenced at the link [42].

Figure 2 represents how the data flows for biometric authentication *after* the installation of the Bio-Guard app. Along with the web version of the app. The web app was installed on apache tomcat with hibernate support and JBoss data services. Data to the central database could be updated

via cookies enabled sessions, using (*representational state transfer*) REST-ful web services. HTML5 markups and bootstrap would display the formatted data. The web App has enriched UI to work with various screen sizes like LDPI (low dots per inch) to XXXH-DPI. It also allows login via Facebook or Google API (application programming interface) to request public fields such as name, gender, user id, and the full name of users, code example of which is referenced at the link [43]

Figure 2. An architectural diagram is showing how biometric authentication works after installing Bio-Guard app on a registered mobile device and Oracle biometric authentication server. The numbers 1a, 1b, 2a to 2d, and 3 to 6, show the sequential steps of data flow.

3.3. System's Requirements

Minimum requirements to run the App on a Smartphone are:

- Depending on the operating system of the device, a Bluetooth and GPS enabled Android OS Version 2.3 and above.
- Internet connection to download and install the app.
- Mobile-network or wi-fi to support browsing, uploading the data to the server, and downloading the data.

3.4. Installation Process of the App

On installation of the server-side of the app, on the host server, it generates "server installation id" (SID), e.g., "sid1234". The complete installation of the client-side of the app has three steps. a) On installation of the client-side of the app on a mobile device, it generates "client installation id"

(CID), e.g., "cid5678," and *this* gets linked to the device id / international mobile equipment identity (IMEI) of the mobile device.

It also creates a "Bio-Guard" icon. b) Then a user needs to register the installation of the app, which links the "app's CID to the user profile and generates a trigger point in the "server-side of the app" to send an OTP to the registered users to verify her/his identity. c) The verification of identity via the OPT confirmation generates another trigger point in the App's server database to send the "SID" to the registered users to complete the installation of the client-side of the app. On a single tap of the "Submit" button of the client-side of the app, as shown in Figure 3, the server receives the linkage of the user's profile with the app's CID and SID and generates another trigger point to send a message about the "installation completion status" to the users.

The screenshot shows the Bio-Guard app's registration interface. At the top, there are two buttons: "g+ Sign in with Google" (red) and "Sign in with Facebook" (blue). Below these is a link "or Create a new Account". The form consists of several rows of input fields: "First Name" and "Last Name", "Date of Birth" and "*Email id", "Mobile Phone" and "Phone", "User ID" and "Password". The "User ID" field contains the text "Biogaurduid1" and the "Password" field contains "*****". Below the form, there are two buttons: "Register to receive OTP" (green) and "Click here to Resend Server" (blue). Below these are two more input fields: "Cofirm OTP to Receive Server" (containing "*****") and "Enter Server Installation id to" (containing "*****"). At the bottom of the form is a large purple "Submit" button. The phone's status bar at the top shows 50% battery and 2:27 PM.

Figure 3. It shows the Bio-Guard app after it expanded on a Samsung android mobile phone screen.

Thus, the user's device gets the company's SID linked to the CID of the app. The combination of "cid1234" and "sid5678" along with user profile and IMEI makes a complex and unique identifier for the user verification. In regular physical biometric authentication, the secret key is stored in the fingerprint sensor and is compared with the secret key stored in the security policy [44]. In the case of the authentication via the "Bio-Guard," app, the combination of SID, CID, and the secret-key stored in the fingerprint sensor is compared with the server-side secret-key stored in the security policy, SID and CID. For the existing users, the user profile of the web application, and that of the app gets in synch. For new users, their profile needs to be first created and verified by the system administrator team before users will receive OTP

3.5. Error Handling

Warning messages, confirmation messages, and exit options have been provided to avoid the program code to fall in an endless loop and hang the application. However, more robust error handling provisions would be required after testing on a broader testbed. For the sake of simulation of an extra layer of biometric security and proof of the concept, the next section focuses on experiments and usability measurements of the app.

3.6. Current Limitations of the App

- Once the Bio-Guard app is connected to an application on the server-side, it will not allow online access without getting SID plus CID.
- For the users who want to login via Windows or Apple iOS, another version of the app is to be developed and installed.

4. Experimentation

The experimentation section has been subdivided into *seven subsections*: 4.1) The methodology of test population sampling; 4.2) Testing environment; 4.3) Performance test of the app; 4.4) Design, functional cum usefulness test on the app; 4.5) Overall usability evaluation of the app on the SUS scale; 4.6) Test for false rejection rate (FRR), false acceptance rate (FAR), and equal error rate (EER); 4.7) National level survey to test the success of the SSABSLM in the realistic hospital environment.

4.1. The Methodology of Test Population Sampling

Testing with Biometric data is a very sensitive issue. It was challenging to find and convince test users and have their profiles in a web-based application. We could engage 110 employees of the project sponsoring organizations whose fingerprint information was already available in the database of the fingerprint-based attendance system (FBAS), for another project. For the cost, convenience, and time effectiveness perspective, *expert/ judgment sampling method* was used so that expertise of selected experienced subjects/ experts could be used to represent the response of a larger unknown population, which was beyond the available resource pool of this project. Judgment sampling is not always preferred but is technically and conceptually the most recommended approach to select useful samples who know about the process, performance, and the impact of changes over a longer period. [45]. *It was assumed that each expert tester/user would represent a response of 10-15 non-expert users.* Thus, the quality of the response from a population of 110 experienced testers with experience in the usage of biometric sensors can be equivalent to about 1100 people without such experience. Moreover, initially, 250 people were interviewed for the experimentation, out of which 200 were selected, but only 110 testers agreed to allow using their biometrics profile in the web application and signed the “*privacy consent form*” (PCF). The testers taken for the experiment were from Mumbai, India- a city that is very cosmopolitan with people from a diverse socio-economic, cultural, and linguistic background. These testers had either a graduate or master's degree in engineering or science. Some of those testers had software development and testing work experience in western countries also.

The survey was conducted at the national level in the patient registration halls of the top-notch hospital environment in 5 major metro cities of India, i.e., Mumbai, Delhi, Chennai, Bangalore, and Kolkata. These hospitals are known to have registrants from many countries who come here as medical tourists for high-quality, low-cost treatments. The original sample population chosen for

screening and interview was 600, of which 450 had experience is the usage of fingerprints and or biometric devices. Out of 450, only 300 agreed to spend time learning the process, sign the “FAP” and take part in the survey. Most of these users had either a graduate or master's degree in science. Thus, this high-quality sample population, 300 users who were screened and interviewed, may be considered to represent about 3000 general population. Remaining demographics, i.e., mean age, the number of males, females, etc. of the sample population is described in the respective experimental situation.

4.2. Testing Environment

This subsection provides some brief background information about the Bio-Guard app and the back-end web-application, which was being accessed by the testers via the app. Like many other applications, this FBAS had three checkboxes in users' profiles to send them alert/ information for verification. One checkbox was for agreeing to the MFA to send a “one-time password” (OTP) for user verification after successful authentication of the password. One checkbox was for sending short text alert via “SMS” on the user's registered mobile number. The third checkbox was for sending a detailed alert message via “email” on the user's registered email address. The sample of SMS and an email notification message is given in *Appendix A*, which can be changed by the system administrator. Users were asked to choose either all the checkboxes and agree to *online agreement of the company about online data privacy* if they wanted those services to get activated on their account. The company also provided an option to opt-out of those services if users wanted to. This paper assumes that the readers already know how an identity verification process works on a standard fingerprint web-application, so, this verification process is not being detailed here.

Before the installation of the “Bio-Guard” app, users could login to the FBAS online remotely using their regular password. Anyone could login to the user account with stolen, UID, and password. Users could login to the FBAS with their fingerprint but were not using it for fear of spoofing and security. Anyone with a spoofed fingerprint could login to the user's profile and change the password and phone number to receive a notification. This was possible much before the user could get to know about it. But once the “Bio-Guard” app is connected to the FBAS, the hacker needs a registered device. A user would not be allowed to use any unregistered “fingerprint-sensor-enabled-mobile (FSEM) device. Users can install the client-side of the “Bio-Guard” app on multiple FSEM, but the number of FSEM devices allowed would be determined in the company's server database by the system administrator.

Moreover, the user would get notification about another FSEM device along with a timestamp, location, and device id of the new device during the app installation process itself. It would help the users to take immediate preventive action by reporting to the system administrator to disable FSEM access and change the password if there is any doubt about that being compromised or lock the account till further verification. It would make the hackers' job more difficult, and users' accounts more secure.

If anyone else tries to use a spoofed fingerprint of the user from a stolen but registered FSEM device, then users would get a notification about another FSEM being used, provided notification

profile is not changed yet. It would help trace the stolen device location, and the user can disable remote login option in the *FBAS* and contact system admin to deregister the stolen *FSEM* device from the server database. It would generate confidence in users to use their mobile devices for biometric authentication.

The app requires a CID linkage to the SID to complete the installation process. Therefore, the complete installation has 3 steps. a) Download and install the setup. It creates an icon “Bio-Guard” on mobile device’s screen, to a single tap, expands and registers the app. b) Fill up relevant data in the fields of the Bio-Guard screen, as shown in Figure 3, to register the app’s CID linked to IMEI. It will connect the user’s profile to the app’s CID and will send the SID to the registered users, on confirmation of OTP. c) Users would single tap the “Submit” button after entering received SID, and on the verification of the SID, users will get notification about the completion of the installation process. After the installation completion via the above three steps, the registered users will get information from the server provided notification option is saved in the user’s profile. The server side of the Bio-guard app can be configured to send notifications about the first installation on a device so that users get a minimal notification if they choose to. Once installation completion status message is received, users can securely login to the web-application connected to “Bio-Guard” either via Biometric id in 1 step or via mobile password plus the OTP received from the application in 2 steps.

4.3. Performance Test of the App

Phan *et al.* [46] proposed a transport protocols-based performance evaluation for mobile apps. Oliveira *et al.* [47] proposed an energy consumption-based method of evaluation for mobile apps. Many users prefer security over performance, and many do the vice-versa. For this reason, we tested the response time and battery consumption performance of the Bio-Guard app.

To achieve the diversity objective for this experiment, we tested the performance on three smartphones of different capacity, in terms of RAM (Random Access Memory) battery power, CPU (Central Processing Unit), and hard disk drive (HDD) [48]. We deliberately chose a legacy, 1 latest and one somewhat older mobile phone to add variety and the year of manufacturing. We chose a legacy phone with a lower capacity to test the backward compatibility of the app. Still, we did not go beyond 2017 because phones older than that may not have very reliable fingerprint sensors. Table 1 shows the relevant specifications.

To test the performance, we deactivated all other apps and ran the Bio-Guard app on a fully charged battery for 30 minutes, allowing maximum possible time, the app may be required to be in use at a time. Mobile phone MP1, consumed 151 milliamper-hour (mAh) energy in 30 minutes which equals to about 3.5 % of the full battery power. Mobile phone MP2 consumed about 11% while MP3 consumed about 6 %, as shown in Figure 4.

Table 1. Mobile phones used in the “Performance Test of the app” and their main relevant features.

Mobile Phones	Year Made in	HDD Capacity	RAM in GB	CPU in GHz	Battery in (mAh)
MP1	2019	32	16	2.3 Octa-core Quad	3000
MP2	2018	16	8	1.4 Quad-Core	2000
MP3	2017	8	4	1.2 Quad-Core	2000

We measured Response time for 3 important functions of the app, i.e., login, minor address update, and closing of the app while WhatsApp was active in the background. The result is shown in Figure 5. The app took maximum response time of 1600 milliseconds (ms) for login by the legacy mobile phone (MP3) and a minimum response time of 800 ms, for minor address update by the latest mobile phone (MP1). As per the experiment, the app's response time seems reasonable, though it may require some improvement based on broader test scenarios.

Figure 4. This figure displays the comparative battery energy consumption of the Bio-Guard app for 30 minutes, on the mobile phones MP1, MP2, and MP3. The X-axis represents duration, in minutes, and the Y-axis represents battery energy consumption in milliamperes-hour (mAh).

Figure 5. This figure displays the comparative response time of the Bio-Guard app for 3 main functions, on mobile phones, MP1, MP2, and MP3. The X-axis represents 3 main functions of login (1), minor address update (2), and closing the app (3). The Y-axis represents response time in milliseconds (ms).

4.4. Design, Functional cum Usefulness Test on the App

Testing with live Biometric data of a large number of people is a very sensitive issue. It was challenging to find and convince many test users. However, we tried our best to make experimental methods as much representative and scientific as feasible in our given circumstances. We could engage 110 employees of the project sponsoring organization, whose fingerprints information was already available in the database of *Fingerprint-Based-Attendance-System* (FBAS), for another project.

The participants had fingerprint access to one of the following android phones, e.g., Samsung Galaxy Note-9, Samsung Galaxy S9, Google Pixel 2 XL, OnePlus 6, Vivo X21 UD, Huawei P20 Pro, HUAWEI HONOR 8 PRO, SONY XPERIA XZ PREMIUM, SAMSUNG GALAXY S8 PLUS, SAMSUNG GALAXY NOTE 8, SAMSUNG GALAXY S7 EDGE, ONEPLUS 5T, and ASUS ZENFONE AR.

The median age of participants was 22.3 years (SD=4.28). There were 4 male (40%) and the remaining female (60%) participants. These test users had previous experience of fingerprint-based web application login.

Table 2. Ten Experimental questions prepared on the format of the SUS Scale but presented in statement format for easy scoring.

ExptQ1) It was easy to install, register, and complete the setup of the app.
ExptQ2) It was difficult to register to the "Bio-Guard" app via Google account.
ExptQ3) Getting the server-side installation id (SID ¹) was quick, on verification of the OTP ² .
ExptQ4) It was difficult to load the app on the screen after a single tap of the "Bio-Guard" icon.
ExptQ5) The visual clarity and alignment of the app on the screen was good and convenient to use after it loaded on a single tap of the "Bio-Guard" icon.
ExptQ6) It was difficult to remotely login to the FBAS ³ application and access the personal profile via the fingerprint sensor of the mobile, after installing the "Bio-Guard" app.
Q7) I felt more confident in the "Bio-Guard" app when I could not login to the FBAS, using the fingerprint sensor of an unregistered mobile.
ExptQ8) I lost confidence in using fingerprint sensors to remotely access my record after I received a notification when I logged in to the FBAS from another mobile device via OTP ² .
ExptQ9) All the box fields and buttons of the "Bio-Guard" app functioned with ease and as expected.
ExptQ10) It was difficult to close the app with a single tap of the "home/ close" button of the mobile device.

¹SID – Server Installation Id, ²OTP-One Time Password, ³FBAS- Fingerprint-based-attendance-System.

To test the comparative functionalities of the app, we prepared ten experimental scenarios on the model of the SUS usability scale [49]. We made one question for each experimental situation and asked users to mark their rating on 5 points Likert scale. *Odd-numbered* experimental items 1, 3, 5, 7, and 9 were *direct questions* and were scored as scale position minus 1. *Even-numbered* items, i.e.,

2, 4, 6, 8, and 10 were *inverted questions* and were scored as 5 minus the scale position. To make the scoring easy, we converted the 10 experimental questions (ExptQ1 to ExptQ10) and presented in the following statement format, as shown in Table 2. The total score of each user was multiplied by 2.5 to convert the overall SUS score to be in the range of 0 to 100.

The test installation set up of the app is loaded to Git Hub and or can be requested by writing an email to the copyright holder mentioned in GitHub [50]. The results were analyzed and interpreted on the model of the SUS score interpretation guide. A SUS score above 68 is considered above average. For example, a raw SUS score of 71 of this experiment converts to a percentile rank of 67% [51].

Before the experimentation, the server-side of the application was already installed, and the installation id was generated, e.g., "SID1234". We asked users to login to the FBAS via physical local fingerprint scanner and select both the checkbox mentioned above to get "SMS" as well as an email alert and save their profile. We gave a printed copy of the sheets of the experimental questions to the group of 110 users, explained to them the scoring pattern, and briefed them on how the app would work. We gave the users a link to download the client-side of the app.

4.4.1. Experiment 1

Was it easy to install, register, and complete the installation process of the "Bio-Guard" app?

Many users may not prefer to use an app that is difficult to set-up. To test the speed and ease of installation of the app, we asked users to connect to the local wi-fi network, download the complete installation set up of the client-side of the "Bio-Guard" app from a web link to get it completely, installed on their smartphones.

To complete the installation process of the app, users performed the following 3 steps. **i)** Users downloaded and installed the client side of the Bio-Guard app, which generated CID and got it linked to the IMEI of their mobile device and also created an icon "Bio-Guard" on the user's mobile. **ii)** Then users single tapped on the "Bio-Guard" icon, expanded the app's screen, entered required data, registered the installation of the Bio-Guard app, to receive OTP, as shown in Figure 3. **iii)** Users then verified their registered identity by confirming the OTP they received. Later, users received SID, entered the SID, tapped of the "Submit" button, and received a message about the "installation completion status."

We had explained the 3-step process to the users to set the expectation right. We requested the users to consider each step as one installation of a regular app while comparing and rating this process of the app. We asked users to rate the ease of installation, as compared to other apps they use, on the scale of 1 to 5 (1 means I strongly agree that installation of the "Bio-Guard" app was easy and 5 means I strongly disagree).

4.4.2. Experiment 2

Was it difficult to register the "Bio-Guard" app via Google account?

For convenience purposes, many users prefer to use their Google or Facebook profiles to login apps. To test this functionality of the app to register via google API, during the installation

process, we requested the users to sign up via their google account to receive the OTP. We then asked them to compare the response time with the response time of other apps when they login to other apps via google account.

We asked users to rate the response time, on the scale of 1 to 5 (1 means I strongly agree that the app was very slow to login via google account and took longer than expected time and 5 means I strongly disagree).

4.4.3. Experiment 3

Was getting the server-side installation id (SID) quick, on verification of the OTP?

Quickly getting the "SID" is a critical criterion to complete the installation process. Therefore, we evaluated the response time performance of the server in sending server-side installation id, on confirmation of the OTP, separately.

After the installation process was completed, as per *experiment 1*, we asked testers to compare the response time in getting the "SID" after they verified the OTP they received, with other such processes they perform for other apps. We asked to rate the response time on the scale of 1 to 5 (1 means I strongly agree that the server's response time in sending SID was reasonably good and 5 means I strongly disagree).

4.4.4. Experiment 4

Was it difficult to load the app on the screen after a single tapping of the "Bio-Guard" icon?

If an installed app does not load quickly to perform its functions, many users would be hesitant to use such an app. To test the loading speed of the app, we asked users to single-tap the "Bio-Guard" icon to load the app get expanded for use on their mobile screen, as shown in Figure 3.

We asked users to rate the loading time as compared to the average loading time of other apps they use, on the scale of 1 to 5 (1 means I strongly agree that the app was struggling to load and took longer than expected time and 5 means I strongly disagree).

4.4.5. Experiment 5

Was the visual clarity and alignment of the app on the screen good and convenient to use after it loaded on a single tap of the "Bio-Guard" icon?

For correct data entry, comfort, and aesthetics, this aspect of the test is crucial. To test the visual alignment and clarity of the app, in the ease of operations, we asked the users to check if the visual clarity of the app after it expanded on the mobile screen on a single tap of the "Bio-Guard" icon, as shown in Figure 3. We requested users to cross-check the field's text, button text, edges of the expanded app on their mobile, and compare it with other test users. We asked testers to make sure that the screen was not truncated on the sides, clear enough, and well-aligned for easy use, on a mobile screen,

We asked users to rate *visual clarity* and *alignment* on the scale of 1 to 5 (1 means I strongly agree that the app's visual clarity and alignment were okay to make it usable and 5 means I strongly disagree).

4.4.6. Experiment 6

Was it difficult to remotely login to the FBAS application and access the personal profile via the fingerprint sensor of the mobile, after installing the "Bio-Guard" app?

The whole purpose of this app is to securely and easily login to a web application with an extra layer of security. This experiment was to test this core functionality. To check the ease of accessing a web application remotely, after adding an extra layer of protection with an app like "Bio-Guard," we asked testers to login via fingerprint sensors of their mobile. Then we asked them to rate the ease of login as compared to other fingerprint-based web app login on the scale of 1 to 5 (1 means I strongly agree that it was difficult to login via the Bio-Guard app and 5 means I strongly disagree).

4.4.7. Experiment 7

Did you feel more confident in the "Bio-Guard" app when you could not login to the FBAS, using the fingerprint sensor of an unregistered mobile?

The purpose of this app is to provide an extra layer of security to the application it is connected to, thus, not allowing remote access to the application without the "Bio-Guard" app. To perform this regression testing, we asked users to login remotely via another mobile device where the "Bio-Guard" app was not installed. Testers clicked on the FBAS icon, which proposed to enter their user id and password, but they could not login. Testers could not login to the online version of the FBAS from a test laptop, either. Then we asked users to rate their confidence level in the security of the Bio-Guard on the scale of 1 to 5 (1 means I strongly agree that login via Bio-Guard is very secure and 5 means I strongly disagree).

4.4.8. Experiment 8

Did you lose your confidence in using fingerprint sensors to remotely access your record after you received a notification when you logged in to the FBAS from another mobile device via OTP?

Getting notification before a hacker can login to a user's account is critical for an alert user. We asked all the 110 users logged off from the current finger-based attendance system and requested them to create their fingerprint profile on 2 test mobiles. "Bio-Guard" client app was already installed on these 2 test mobiles with fingerprint sensors. Then we requested them to login to their finger-based attendance system using the fingerprint sensor of the test mobile. We asked them to check their personal mobile for alert they received. They all got notification messages, as mentioned in Appendix A, that "someone logged in to your account in the FBAS from another device." Then we asked the testers to rate their confidence level in the usage of fingerprint devices remotely, on the scale of 1 to 5 (1 means I strongly agree to have lost confidence in using fingerprint sensors, to remotely access a web-application and 5 means I strongly disagree).

For *privacy and security reasons*, we asked the testers to delete their fingerprint profiles from these 2 test mobiles after the test.

4.4.9. Experiment 9

Did all the box fields and buttons of the “Bio-Guard” app function with ease and as expected?

Everyone wants to use the app without any bug, so getting the input of users about the functioning of the app was important. At the time testing this aspect of the app, users had experienced the operation of almost all buttons and boxes of the app.

So, we asked users to rate the overall ease of operation of the app’s buttons and boxes on the scale of 1 to 5 (1 means I strongly agree that the app’s fields and buttons were easy to operate and 5 means I strongly disagree).

4.4.10. Experiment 10

Was it difficult to close the app with a single tap of the “home/ close” button of the mobile device?

People use mobile devices for multiple applications. The Bio-Guard app should not hog all the memory and computing power of the device forever, just for extra security. To test the closure of the app and without it interfering with other regular functions of the mobile, we asked the test users to single-tap the “home” button of their smartphone while the app was loaded, and its expanded screen was visible on their mobile’s screen. We asked users to rate the closure time of the app as compared to the average closing time of other apps they use, on the scale of 1 to 5 (1 means I strongly agree that app was struggling to close and took longer than expected and 5 means I strongly disagree).

Figure 6. This Box Plot displays the comparative average score of the Bio-Guard app on the SUS Scale and the scale prepared on the pattern of the SUS scale, for 110 experiments. The X-axis represents 110 expert test users, and the Y-axis represents the comparative score.

The comparative score on the SUS scale questions and that of the 10 experimental questions prepared on the format of the SUS scale is plotted in the boxplot, as shown in Figure 6.

4.5. Overall Usability Evaluation of the App on the SUS Scales

At the end of the ten experimental scenarios mentioned in B), we gave the users an hour of break. We then collected their responses on the actual SUS questions to get the overall usability of the app.

At the end of the ten experimental scenarios, we gave the users an hour of break and then presented with actual SUS questions, to get the overall usability of the app. The average and standard deviations of the response score on the original SUS scale and that of the test scale prepared for the Bio-Guard app, on the pattern of the SUS scale are displayed in Table 3, and presented in result analysis section 5, to draw inferences from this table.

Table 3. A comparative score of the standard SUS Scale and 10 Experiments.

Average/Mean SUS rating score of 110 Users	71.2
Average/Mean Experimental rating score on 110 users on SUS modeled experiment, performed for the Bio-Guard app	73.95
Std Dev of SUS rating score of 110 Users	4.342
STD Dev Experimental rating score on 110 users on SUS modeled experiment, performed for the Bio-Guard app	5.941

A comparative rating score of the standard SUS scale and 10 experiments performed for the Bio-Guard app, presented and rated on the model of the SUS scale for 110 expert test users.

4.6. Test for False Rejection Rate (FRR), False Acceptance Rate (FAR), and Equal Error Rate (EER)

As per the guidelines of Robertas *et al.* [24], Jorgensen and Yu [52], we tested the app for False Rejection Rate (FRR), False Acceptance Rate (FAR), Equal Error Rate (EER). A lower EER means a more accurate application system. To reduce training time, we conducted this test after we conducted usability tests.

While FAR and FRR tells if the app correctly identified the subject. The EER specifies the values at which FAR and FRR become almost equal. The metrics were calculated as follows:

$$FRR = FR / AA$$

$$FAR = FA / IA$$

Here FR (False Rejections) is the number of falsely rejected verification attempts of a valid subject, and AA (Authorized Attempts) is the total number of authorized attempts. FA (False Acceptance) is the number of the falsely accepted claims of an impostor as a genuine user. IA

(Impostor's Attempts) is the number of imposter's attempts. The test yielded a mean FAR, FRR value of 0.4200, and 0.3600, respectively. The resultant EER is 0.0600, as shown in Figure 7.

Figure 7. This figure displays the ERR at the intersection of FAR and FRR. The X-axis represents the similarity threshold, and the Y-axis represents Error. In this case, at the similarity threshold of 54, the resultant ERR is 0.06.

4.7. National level Survey to Test the Success of the SSABSLM in Realistic Hospital Environment

A national-level survey was conducted on a *sample population of 300 users* in the realistic patient registration hall setting of the project sponsoring hospital and its partners, using recorded video clips of the tests A), B) & C) [53]. The median (MD) age of participants was 25.3 years, with a standard deviation (SD) of 3.48. There were 120 males (40%) and the remaining 180 female (60%) participants. Some of these users, including the 100 testers of experiments A), B), and C), plus 200 additional potential users of the app, had previous experience of fingerprint-based web application login. For privacy reasons and to protect the identity of the testers, the video clip of the recorded test used for this survey is not being made public but may be received from the project sponsoring organization.

Table 4. Survey questions to test the success of the SSABSLM.

1) I felt more confident to use web-based applications via biometric devices when I saw that the testers could not login to the FBAS using the fingerprint sensor of an unregistered mobile device.
2) The concept of getting the server-side installation id (SID) only on the verification of the OTP is very useful for prompt preventive action.
3) I think with this kind of “add-on” extra layer of security the biometric technologies can be more convenient and reliable than password-based access systems.
4) I think SSABSLM can make access to personal information more secure.
5) After watching the performance of the Bio-Guard app, I think SSABSLM can be useful for many groups of people.

We explained the experimental details to the users and then showed the video recorded for tests A), B) & C). They responded to the survey questions, as shown in Table 4, on a 5-point Likert scale for the “server-specific “add-on” biometric security model (SSABSLM) to enhance the usage of biometrics. The cumulative columnar bar graph, as shown in Figure 8, displays the survey results.

Figure 8. This cumulative columnar bar graph displays the response of survey results of 300 expert users for the success of the SSABSLM. The X-Axis shows Survey Question (1 to 5). The Y-Axis displays the number of users who have responded on the Likert from strongly agree to disagree strongly.

5. Analysis of the Experimental Outcomes and National level Survey Results

Experimental scores of the above tests were recorded, normalized, and the results are presented below.

Figure 4 shows that the Bio-Guard app consumed an average of about 7% of the battery power when it ran alone for 30 minutes. So, from the power/energy consumption perspective, it seems reasonable. However, it may require some improvements after testing in more situations.

Figure 5 shows that the average response time of the Bio-Guard app is approximately 1200 milliseconds per transaction, while WhatsApp was running in the background. This response time seems okay for a new app; however, more tests may be required on a broader testbed, to give a decisive conclusion about it.

The mean FAR, FRR value of 0.4200, and 0.3600, respectively, resulted in the *EER* is 0.0600 (6%) at the similarity threshold of 54, as can be seen in Figure 7. At the higher threshold, the ERR could be lowered, but in that case, FRR could have gone up. So, to maintain a balance, the threshold was kept at 54%, and it resulted in slightly higher ERR. The *EER* is reasonably low but needs further balancing and reduction.

The SUS score between 70 and 80 is better than the average [54]. As per Table 3, the average SUS score of the Bio-Guard app is 71.2. The average rating score of 10 experiments performed on the pattern of the SUS scale for the Bio-Guard app has a value of 73.95. Both these results point that the app's functionalities and performance are in an acceptable range, though the overall usability of the app is rated higher. The results also point towards the possibility of improving the app's usability by enhancing some of its functionalities.

The comparative SUS score and the rating score of 10 experiments modeled on the SUS scale, as shown in the box plot graph Figure 6, indicate that the fluctuation in the score was user-specific. In other words, the users who scored higher on the SUS modeled experiment scored high on SUS usability also. This also indicates that the usability rating is a dependent function of such factors as how techno-savvy the users are or how efficient their smartphones are. It implies that with some practice and training, the scores can be enhanced.

The standard deviation of 4.34 for the app on the original SUS scale and the standard deviation of 5.94 on the experiments prepared on the pattern of the SUS scale is on the little higher side. It can be because of the higher ratio of female participants in the test sample.

It can also be a result of socio-cultural effects on the perception of participants as to how comfortable they feel with biometric technology. Some more experiments on broader testbeds should help reduce the deviation by a few points.

The majority of users of the population sample have scored around 70 on both the scales. It is a kind of the middle of the SUS scale. The users who have a high score on SUS Scale also have a high score on the scale prepared for 10 experiments performed on the pattern of the SUS scale for the Bio-Guard app, as shown in boxplot Figure 6. It indicates that the personality of users taking these tests and their socio-economic background may influence the acceptance of biometric technologies. For example, some users may be early adopters and high-risk takers, while others may be low risk-takers.

The survey results for the success of SSABSLM mentioned in D), as shown in the cumulative columnar bar graph, Figure 8, help extrapolate the following information:

a) Question 1: 86% (258 out of 300) of the users agreed that they felt more confident to use web-based applications via biometric devices when they saw that the testers could not login to the FBAS using the fingerprint sensor of an unregistered mobile device, (MD:4.5, SD: 1.04).

b) Question 2: 83% (249 out of 300) of the users responded as agreed and strongly agreed that the concept of getting the server-side installation id (SID) on the verification of the OTP is very useful for prompt action, (MD: 5, SD: 1.16).

c) Question 3: 71.33% (214 out of 300) of the users responded as agreed and strongly agreed that with this kind of "add-on" extra layer of security, biometric technologies could be more convenient and reliable than password-based access systems, (MD: 4, SD: 1.22).

d) Question 4: 86.66% (260 out of 300) of the users as responded agreed and strongly agreed that the SSABSLM could make access to personal information more secure, (MD: 4, SD: 0.99).

e) Question 5: 76.66% (230 out of 300) of the users responded as agreed and strongly agreed that the SSABSLM could be useful for many groups of people (MD: 4, SD: 1.21).

f) Overall, the survey result for the success of SSABSLM is very favorable, with an average of 80.66% of the testers responding as agree and strongly agree for the above five survey questions.

6. Discussion on Implementation Opportunities and Challenges

Like any other novel solution framework, the successful implementation of SSABSLM can provide many opportunities and may face a few challenges, as discussed below. The framework has a high potential to provide the opportunities of SSO (Single-Sign-on) with an “add-on” extra layer of security, especially for the healthcare industry. Increased sense of security in the usage of web-applications can influence the deeper level of cognition to learn and to adapt to new challenges.

6.1. Training, Awareness and Adaptation Challenges

So far, we had the opportunity to develop and test the framework with android based devices. Its development, deployment, and testing on a broader sample population for iOS and Windows may face new challenges. People, especially in developing countries, need to be aware of newly available tools to be trained on.

6.2. Security and Privacy Challenges

The sense of security and confidence in new tools is many times perceptual. The purpose of this framework is to encourage higher usage of biometric technologies, but like other new models, it may take some time to build trust and confidence in the capabilities of this framework.

7. Conclusion and Future Perspectives

Based on the information analysis and the review of relevant literature and reports, biometrics seems to be one of the most useful technologies for multifactor authentication to verify the user's identity, for data security. With the fast growth of biometrics, as “BaaS” (biometric applications as service), in the cyber-society, especially for the usage with IoT devices and related security vulnerabilities, it has gone high on the radar of many companies [55].

The literature review also indicates that because of the *low usage rate* of biometrics, many organizations, especially small and medium segment healthcare companies, are not finding it very *cost-effective* to invest in robust biometric systems. Since many of them lack dedicated fraud prevention and security teams, they are becoming vulnerable to cyber hackers. Therefore, the usage rate of biometrics must be increased to achieve the economy of the scale.

The architecture, design, flow diagrams, logic, the functional, operational aspect of the framework seems logical as an “add-on” for an extra layer of security to biometric-based web-applications. The experimental results on battery performance, response time, regression tests of accessing web apps, seems to have generated confidence in the testers. A reasonably low *Equal Error Rate (EER)* of 6% and a score of 71% on the usability scale indicates the authenticity of the app as a testing tool. The survey for the success of “server-specific add-on biometric security layer model (SSABSLM),” has a very favorable score of 80%.

The experimental outcomes of the biometric mobile app and subsequent survey for the success of the SSABSLM show a reasonable potential of this kind of “add-on” layer of biometric security in snowballing the participation of users in the usage of biometrics. Higher usage rates may make deployment of biometrics more cost-effective for many organizations to decrease their information security risk. However, the SSABSLM must overcome a few challenges related to training, adaptation, and socio-cultural data privacy norms.

8. Patents

There is a pending patent for this app.

Author Contributions:

Bhanu Singh is the primary author of this research who conceptualized, conceived, and designed the mobile app software and experiments. Nirvisha Singh performed project administration, data analysis, investigation, validation, and provided suggestions to improve the paper. Both the authors were involved in experiments, data curation, review, and approval of the final manuscript.

Funding: This work was supported in part by a joint pilot project between Nishaan Infotech US LLC, Nishaan Infotech India Pvt. Ltd., and Lifeline Hospital, Mumbai, Maharashtra, India. Some of the information is covered under the confidentiality agreement, so, the permission of the above three organizations would be required with reference project number LLHMHI.proj.852019. However, this article is not funded by any organization.

Acknowledgments: The author is very thankful to the anonymous reviewers and colleagues who provided insightful thoughts, valuable suggestions, and encouragement. The author is also grateful to Ms. Jo Quintanilla, University of Sydney, Australia, a digital project manager by profession and Ms. P. Singh, Bombay University, India, for organizing information and proofreading the papers. The author remains the only person accountable for any omissions or mistakes.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

1. The SMS short message alert of the “Bio-Guard” app:

A security alert from the company” abcd123” employee id ending xxx55.

Dear Mr./Ms. Abc.Xyz

We are letting you know that your employee record was accessed using device id, location ABC on date dd.mm.yyyy at hh.mm.ss(time).

If you don't recognize this activity or want to review your account activity, please check your registered email for details or contact your system admin team.

822 2. *Detailed email alert message of the “Bio-Guard” app:*

823 A security alert from the company “abcd123” employee id ending xxxxx55.

824 Dear Mr./Ms. Abc.Xyz

825 We are letting you know your employee record was accessed using device id, location ABC on date
826 dd.mm.yyyy at hh.mm.ss(time).

827 If you don't recognize this activity or want to review your account activity, go to www.abcdefg.com
828 or contact your system admin team.

829 *Remember:* We never ask for personal information such as employee id, card PIN, or social security
830 number or Tax-ID, driving license number, etc. in emails. However, if you think an email is
831 suspicious, don't click on any links. Instead, forward it to www.abcdefg.com and delete it.

832 Please note that you are receiving this email as per your selection choice and service agreements,
833 whether or not you elect to receive such alerts. Read our privacy notice and don't reply directly to
834 automatically generated messages. Abcd Ltd. © 2019, all rights reserved. This email was sent to
835 abc.xyz.123@gmail.com.

836 References

- 837 1. Vincent Bonneau, IDATE and Laurent Probst, Virginie Lefebvre, PwC. *Digital transformation monitor*
838 *biometrics technologies: a key enabler for future digital services*. January 2018. Available online:
839 [https://ec.europa.eu/growth/tools-databases/dem/](https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Biometrics%20technologies_v2.pdf)
840 [monitor/sites/default/files/Biometrics%20technologies_v2.pdf](https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Biometrics%20technologies_v2.pdf)
841
- 842 2. Gavrilova, Marina L. *Biometric-based authentication for cyberworld security: challenges and opportunities*, (2014).
843 Canadian Defence & Foreign Affairs Institute, ISBN: 978-0-9737870-9-2.
844 Available online: <https://pdfs.semanticscholar.org/baf7/47463f7a4864a9e469b16839a0184eb5d621.pdf>
845
- 846 3. Luana Pascu. *Sentara healthcare integrates Imprivata biometric patient identification technology*, Nov 21, 2019.
847 Copyright © 2020 Biometrics Research Group, Inc. Available online:
848 [https://www.biometricupdate.com/201911/sentara-healthcare-integrates-imprivata-biometric-patient-](https://www.biometricupdate.com/201911/sentara-healthcare-integrates-imprivata-biometric-patient-identification-technology)
849 [identification-technology](https://www.biometricupdate.com/201911/sentara-healthcare-integrates-imprivata-biometric-patient-identification-technology)
850
- 851 4. *Identity & access management - Global Market Outlook (2016-2022)*, last accessed December 2019. Copyright ©
852 1999-2020, MarketResearch.com. Available online: [https://www.marketresearch.com/Statistics-market-](https://www.marketresearch.com/Statistics-market-research-consulting-v4058/identity-access-management-global-outlook-10771731/)
853 [research-consulting-v4058/identity-access-management-global-outlook-10771731/](https://www.marketresearch.com/Statistics-market-research-consulting-v4058/identity-access-management-global-outlook-10771731/)
854
- 855 5. Chris Burt. *Mastercard taps biometrics and behavioral analytics in new product suite for healthcare partners*, Oct
856 28, 2019. Copyright © 2020 Biometrics Research Group, Inc. Available online:
857 [https://www.biometricupdate.com/201910/mastercard-taps-biometrics-and-behavioral-analytics-in-new-](https://www.biometricupdate.com/201910/mastercard-taps-biometrics-and-behavioral-analytics-in-new-product-suite-for-healthcare-partners)
858 [product-suite-for-healthcare-partners](https://www.biometricupdate.com/201910/mastercard-taps-biometrics-and-behavioral-analytics-in-new-product-suite-for-healthcare-partners)
859
- 860 6. Katrine Spirina. *Biometric authentication: The future of IoT security solutions*, July 05, 2018. Copyright © 2020
861 IoTEVOLUTIONWORLD. Available online: [https://www.iotevolutionworld.com/iot/articles/438690-](https://www.iotevolutionworld.com/iot/articles/438690-biometric-authentication-future-iot-security-solutions.htm)
862 [biometric-authentication-future-iot-security-solutions.htm](https://www.iotevolutionworld.com/iot/articles/438690-biometric-authentication-future-iot-security-solutions.htm)
863

7. C. Hongsong, F. Zhongchuan, and Z. Dongyan. *Security and trust research in m2m system, in vehicular electronics and safety (ICVES)*, 2011 IEEE International Conference on. IEEE July 2011, pp. 286–290. DOI:10.1109/ICVES.2011.5983830. Available online: <http://ieeexplore.ieee.org/document/5983830/>
8. G. M. Køien. *Reflections on trust in devices: an informal survey of human trust in an internet-of-things context*, *Wireless personal communications*, Dec 2011, vol. 61, no. 3, pp. 495–510. DOI:10.1007/s11277-011-0386-4
9. Mohamed Abomhara and Geir M. Køien. *Cybersecurity and the Internet of Things: vulnerabilities, threats, intruders and attacks*. Journal of Cyber Security, Vol. 4, 65–88. 2015, River Publishers. DOI: 10.13052/jcsm2245-1439.414,
10. *Top software failures in recent history*, Aug 7, 2019; Copyright © 2019 IDG Communications Ltd; Available online: <https://www.computerworld.com/article/3412197/top-software-failures-in-recent-history.html>
11. Charles Arthur. *iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club*. The Gaurdian, 23 Sep 2013. Available online: <https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked>
12. *Hacking responsible for 83% of breached healthcare records in January*. HIPAA Journal, Last modified March 1, 2018. Available online: <https://www.hipaajournal.com/hacking-responsible-83-breached-healthcarerecords-january>.
13. Fred O' Connor. *What happens if your biometrics are stolen?*, November 6, 2019. Copyright 2020, Veridium Ltd, UK. Available online: <https://www.veridiumid.com/blog/biometric-mythbusters-stolen-fingerprints-mean-identity-theft/>
14. Jeffrey Cheng. *Securing IP surveillance cameras in the IoT ecosystem*. Trend Micro IoT Security, 18 April 2018. Available online: <https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/securing-ip-surveillance-cameras-in-the-iot-ecosystem>
15. W. Meng, D. S. Wong, S. Furnell, and J. Zhou. *Surveying the development of biometric user authentication on mobile phones*, in IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1268–1293, third quarter of 2015. DOI: 10.1109/COMST.2014.2386915
16. Y. Chen, J. Sun, R. Zhang, and Y. Zhang. *Your song your way: rhythm-based two-factor authentication for multi-touch mobile devices*, 2015, IEEE conference on computer communications (INFOCOM), Kowloon, 2015, pp. 2686–2694. DOI: 10.1109/INFOCOM.2015.7218660
17. Ferrag, M.A., Maglaras, L., Derhab, A. et al. *Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues*. Telecommun Syst 73, 317–348. February 2020. Available online: <https://doi.org/10.1007/s11235-019-00612-5>
18. D. He, J. Bu, S. Chan, C. Chen, and M. Yin. *Privacy-preserving universal authentication protocol for wireless communications*, in IEEE Transactions on Wireless Communications, vol. 10, no. 2, pp. 431–436, February 2011. DOI: 10.1109/TWC.2010.120610.101018
19. W. Li, Q. Gu, Y. Zhao and P. Wang. *Breaking two remote user authentication systems for mobile devices*, 2017, IEEE 3rd international conference on big data security on cloud (big data security). IEEE international conference on high performance and smart computing (HPSC), and IEEE international conference on intelligent data and security (IDS), Beijing, 2017, pp. 37–42. DOI: 10.1109/BigDataSecurity.2017.34
20. Traore, I.; Woungang, I.; Nakkabi, Y.; Obaidat, M.S.; Ahmed, A.A.E.; Khalilian, B. *Dynamic sample size detection in learning command-line sequence for continuous authentication*. IEEE Trans. Syst. Man Cybern. 2012, 42, 1343–1356.

21. Mondal, S.; Bours, P. *Continuous authentication in a real-world setting*. In Proceedings of the 2015 eighth international conference on advances in pattern recognition (ICAPR), Kolkata, India, 4–7 January 2015; pp. 1–6.
22. Buduru, A.B.; Yau, S.S. *An effective approach to continuous user authentication for touch screen smart devices*. In Proceedings of the 2015 IEEE international conference on software quality, reliability, and security (QRS), Vancouver, BC, Canada, 3–5 August 2015; pp. 219–226.
23. Mondal, S.; Bours, P. *Continuous authentication, and identification for mobile devices: combining security and forensics*. In Proceedings of the 2015 IEEE international workshop on information forensics and security (WIFS), Rome, Italy, 16–19 November 2015; pp. 1–6.
24. Robertas Damaševičius, Rytis Maskeliūnas, et al. *Combining Cryptography with EEG Biometrics*. Hindawi, volume 2018. Article ID 1867548, <https://doi.org/10.1155/2018/1867548>
25. Guannan Wu, Jian Wang, Yongrong Zhang and Shuai Jiang. *A continuous identity authentication scheme based on physiological and behavioral characteristics*. MDPI, Sensors 2018, 18(1), 179; Available online: <https://doi.org/10.3390/s18010179>
26. Bamasag, O.O.; Youcef-Toumi, K. *Towards continuous authentication in the Internet of Things based on secret Sharing Scheme*. In Proceedings of the WESS'15: Workshop on embedded systems security, Amsterdam, The Netherlands, 4–9 October 2015; pp. 1–8.
27. S. Vhaduri and C. Poellabauer. *Multi-modal biometric-based implicit authentication of wearable device users*, in IEEE Transactions on Information Forensics and Security, vol. 14, no. 12, pp. 3116–3125, Dec. 2019. DOI: 10.1109/TIFS.2019.2911170
28. Li, Stan Z., Jain, Anil. *Encyclopedia of Biometrics*, Chapter *Passive Biometrics*, Pages 46–65. 2009, Springer US, Boston, MA. DOI: https://doi.org/10.1007/978-0-387-73003-5_541
29. Olanrewaju, L., Oyebiyi, O., Misra, S. et al. *Secure ear biometrics using circular kernel principal component analysis, Chebyshev transform hashing and Bose–Chaudhuri–Hocquenghem error-correcting codes*, January 2020, Available online: <https://link.springer.com/article/10.1007%2Fs11760-019-01609-y>
30. Robertas Damaševičius, Rytis Maskeliūnas, Algimantas Venčkauskas, and Marcin Woźniak. *Smartphone user identity verification using gait characteristics*, MDPI, Symmetry 2016, volume 8, issue 10. <https://doi.org/10.3390/sym8100100>
31. Spanakis, E. G., Spanakis, M., Karantanas, A., & Marias, K. (2016). *Secure access to patient's health records using SpeechX Rays, a multi-channel biometrics platform for user authentication*. In Proceedings of the annual international conference of the IEEE Engineering in Medicine and Biology Society, 2541–2544.
32. Spanakis, M., Manikis, G., Porwal, S., & Spanakis, E. G. *Developing a context-dependent tuning framework of multi-channel biometrics that combine audio-visual characteristics for secure access in the eHealth platform for osteoarthritis management*, (2017). In Proceedings of 7th EAI International Conference on Wireless Mobile Communication and Healthcare.
33. Larcher, A., Lévy, C., Matrouf, D., Bonastre, J. F., Tresadern, P., & Cootes, T. (2012). *Bi-modal person recognition on a mobile phone: using mobile phone data*. In 2012 IEEE International Conference on Multimedia and Expo Workshops, pp. 635–640. DOI:10.1109/ICMEW.2012.116
34. Manikis, Georgios C., Marios Spanakis, and Emmanouil G. Spanakis. *Personalized mobile eHealth services for secure user access through a multi-feature biometric framework*. IJRQEH 8.1 (2019): 40–51. Web. 14 Mar. 2020. DOI:10.4018/IJRQEH.2019010104

35. Zahid Syeda, Jordan Helmick, Sean Banerjee, Bojan Cukic. *Touch gesture-based authentication on mobile devices: The effects of user posture, device size, configuration, and inter-session variability*. Journal of Systems and Software, Volume 149, March 2019, Pages 158-173. DOI:10.1016/j.jss.2018.11.017
36. Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin et. al. *Authentication Protocols for Internet of Things: A comprehensive survey*, Volume 2017, Hindawi. Article ID 6562953, <https://doi.org/10.1155/2017/6562953>
37. Gavrilova, Marina L., and Maruf Monwar. *Multimodal biometrics and intelligent image processing for security systems*. IGI Global, 2013. 48-148. Web. 14 Mar. 2020. DOI:10.4018/978-1-4666-3646-0
38. *Using the fingerprint certificate mapper*, last accessed June 2019. Copyright © 2020, Oracle and its affiliates. Available online: <https://docs.oracle.com/cd/E19476-01/821-0506/using-fingerprint-cert-mapper.html>
39. *Device fingerprinting and identification*, Oracle adaptive access manager (OAAM). Last accessed June 2019. Copyright © 2020, Oracle and its affiliates. Available online: https://docs.oracle.com/cd/E40329_01/admin.1112/e60557/finger.htm#AAMAD6186
40. T. K. Roy and T. Kanti Roy. *Fingerprint acquisition & verification on mobile devices*, 2018. International conference on computer, communication, chemical, material, and electronic engineering (IC4ME2), Rajshahi, 2018, pp. 1-5. DOI: 10.1109/IC4ME2.2018.8465605
41. Jain, Anil K, and Arun Ross. *Bridging the gap: from biometrics to forensics*. Philosophical transactions of the Royal Society of London. Series B, Biological sciences vol. 370,1674 (2015): 20140254. DOI:10.1098/rstb.2014.0254
42. Juned Mughal. *How to get current GPS coordinates location android programmatically*, December 2016. Copyright, Android-Examples.com. Available online: <https://www.android-examples.com/get-current-gps-coordinates-location-android-programmatically>.
43. Juned Mughal. *How to get Facebook login user data ID, first name, last name, email, gender, link, locale and account verified status programmatically*, May 2017. Copyright, Android-Examples.com. Available online: <https://www.android-examples.com/facebook-login-graph-api-get-user-info>.
44. *Configuring identix biometric authentication*, last accessed March 2019, Oracle Corporation (1999). Available online: https://docs.oracle.com/cd/F49540_01/DOC/network.815/a67766/07_ident.htm
45. Rocco J. Perla, EdD; Lloyd P. Provost, MS. *Judgment sampling: a health care improvement perspective*. Wolters Kluwer Health Lippincott, Williams & Wilkins. Q Manage Health Care, vol. 21, No. 3, page 170, 2012. DOI: 10.1097/QMH.0b013e31825e8806
46. K. A. Phan, Z. Tari, and P. Bertok. *A benchmark on SOAP's transport protocols performance for mobile applications*, in Proc. ACM Symp. Appl. Comput., 2006, pp. 1139–1144. DOI: 10.1145/1141277.1141548
47. W. Oliveira, R. Oliveira, and F. Castor. *A study on the energy consumption of android app development approaches*, in Proc. 14th IEEE/ACM Int. Conf. Min. Softw. Repositories, 2017, pp. 42–52. DOI: 10.1109/MSR.2017.66.
48. Tourism Mobile App M. Afzaal, M. Usman and A. Fong. *Tourism mobile app with aspect-based sentiment classification framework for tourist reviews*, in IEEE Transactions on Consumer Electronics, vol. 65, no. 2, pp. 233-242, May 2019. DOI: 10.1109/TCE.2019.2908944
Available online: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8680692&isnumber=8695889>
49. Brooke, J. *SUS: A quick and dirty usability scale*, (1996). P.W. Jordan, B. Thomas, B.A. Weerdmeester & I.L. McClelland (Eds.), Usability Evaluation in Industry. London: Taylor & Francis.

50. Nishaan Bio-Guard_Biometrics_app, 2019. Copyright: GitHub, Inc., 2019. Available online: https://github.com/NishaanGHac/Bio-Guard_Biometrics_app
51. Jeff Sauro, Ph.D., ME. *Assuring usability with the system the system usability scale (SUS)*, February 2, 2011. Available online: <https://measuringu.com/sus/>
52. Z. Jorgensen and T. Yu. *On mouse dynamics as a behavioral biometric for authentication*, in Proceedings of the 6th international symposium on information, computer and communications security, ASIACCS 2011, pp. 476–482, China, March 2011.
53. D. Lee, J. Park, and M. Song. *An app-based authoring system for personalized sensory stimulation of children with developmental disabilities*, in IEEE Access, vol. 5, pp. 10583-10593, 2017. DOI: 10.1109/ACCESS.2017.2712123, Available online: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7938615&isnumber=7859429>
54. Aaron Bangor, Ph.D., CHFP, Philip Kortum, Ph.D., James Miller, Ph.D. *Determining what individual SUS scores mean: Adding an adjective rating scale*. JUS Journal Usability Study. Vol. 4, issue 3, May 2009, pp. 114-123. Available online: <https://uxpajournal.org/determining-what-individual-sus-scores-mean-adding-an-adjective-rating-scale/>
55. Stamford, Conn. *Gartner identifies the top 10 Internet of Things technologies for 2017 and 2018*, February 23, 2016. Available online: <https://www.gartner.com/en/newsroom/press-releases/2016-02-23-gartner-identifies-the-top-10-internet-of-things-technologies-for-2017-and-2018>.

© 2020 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).