International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

"Verbal Authentication for Personal Digital Assistants"

Aishwarya Badamgatti[1], Pooja waghmare[2], Pranali korgaonkar[3], Prof. Harish Barapatre[4]

[1,2,3]Final Year student, Department of Computer Engineering,
[4]Assistant Professor, Department of Computer Engineering, Y.T.I.E.T, Karjat, Maharashtra, India

---

Abstract: Personal Digital Assistant (PDA) i.e. a handheld device interacting with human beings verbally and performing tasks that are usually performed by an assistant, has been a growing and continuously evolving technology in recent years. Technology is rapidly automating all the manual work. In such scenario, the concept of PDA where everyone can carry their very own assistant in their pockets and can use it anytime and anywhere without even having to reach their pockets (i.e. completely hands-free usage) proves out to be a great success for technological world. There is no doubt about the fact that PDAs are the future of technology as all the major tech giants like Google, Microsoft, Apple etc. are keen on building and developing their own PDA. Thus, this advancement, demands for a reliable verbal authentication measure where a user can authenticate himself just by talking to the system. Moreover, this conversation should be such that, no intruder or attacker must be allowed to bypass the system even if he listens to the conversation that took place between the user and the PDA. This paper focuses on the security mechanisms that can be used to develop a base for verbal authentication and how it can be used as a powerful tool for validating login for device.

Keywords: PDA - Personal Digital Assistant, STT - Speech to Text, TTS- Text to Speech, API - Application Program Interface.

I. INTRODUCTION:

A Personal Digital Assistant (PDA), also known as a handheld PC, or Personal Data Assistant, is a mobile device that functions as a personal information manager. Most PDAs can synchronize their data with applications on a user's mobile. Hence it can synchronize the user's data like events, birthday, reminders, alarms etc. And use this data to notify the user about it. It is not only restricted to this, since the main aim of PDA is to use it hands free, the user not only set reminders and alarms without using hands, but also perform multitask simultaneously like cooking and reading the notifications, or driving and getting the directions verbally without looking at the device etc. Personal Digital Assistants requires complete shift from textual data feeding to verbal data feeding. In other words, the manual work of feeding the data by typing must be transformed into simple voice commands where data is feed into the system verbally .This implies that, all the security and authentication measures must also be done over voice i.e. verbally. Thus, the authentication mechanism must not be the same for every login unlike standard textual password authentication process where the same textual password is required for every login.

1. TYPES OF PDA DEVICES:

Traditional PDA: Today's traditional PDAs are descendants of the original Palm Pilot and Microsoft Handheld PC devices. Palm devices run the Palm OS (operating_system), and Microsoft Pocket PCs run Windows Mobile. The differences between the two systems are fewer than in the past.

1) **Palm PDA:** Most Palm devices are made by palmOne, which offers the Zire and Tungsten product lines. The company formed in 2003 when Palm Computing acquired Handspring, Inc. Sony, which produced the Palm-based CLIE, stopped producing PDAs in 2005.

2) **Smartphones**: A smartphone is either a cell phone with PDA capabilities or a traditional PDA with added cell phone capabilities, depending on the form factor (style) and manufacturer. Characteristics of these devices include:

- A cellular service provider to handle phone service (As with cell phones, you typically purchase a cellular plan and smart phone from the service provider.)
- Internet access through cellular data networks
- Various combinations of cell phone and PDA features, depending on the device (for example, not all smart phones offer handwriting-recognition capabilities)

2. GOALS AND OBJECTIVES:

A smartphone is considered to be the combination of the traditional PDA and cellular phone, with a bigger focus on the cellular phone part. These handheld devices integrates mobile phone capabilities with the more common features of a handheld computer or PDA. To design a user authentication system with a set of secret questions created based on the data of users short-term Smartphone usage. The main focuses on the security mechanisms that can be used to develop a base for verbal authentication and how it can be used as a powerful tool for validating login for device.

3. LIMITATIONS OF EXISTING SYSTEM:

In this mechanism the user needs to speak out the password or pin or the characters of the string. It is one of the less secure systems, as this works best in the scenario when the

user is alone, or in private place. But if the user is in public or in crowded environment, then people around the user can hear the password. This could lead to easy bypassing the system once a person hears the password. In this mechanism the user's speech pattern and the voice frequency comes into picture for authentication. The existing system uses two main methods for security and both the mechanisms have certain limitations. i.e. Verbal Password & Verbal Recognization

DISADVANTAGES:

- PDA's are Fragile and Delicate to use
- PDA's are Expensive include their cost of purchase & upgrades & cost of maintenance
- PDA's are Limited in Scope

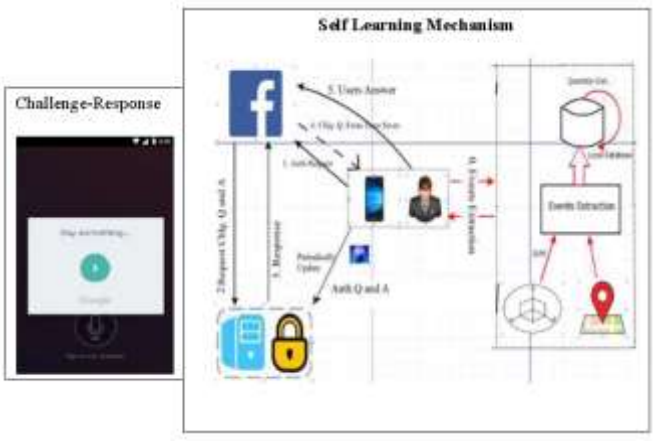
Few examples of PDAs of well-known companies are as follows:

- GOOGLE NOW by Google
- SIRI by iPhone
- CORTANA by Microsoft
- ECHO and ALEXA by Amazon
- MOTO VOICE by Motorola

II. PROBLEM DEFINATION:

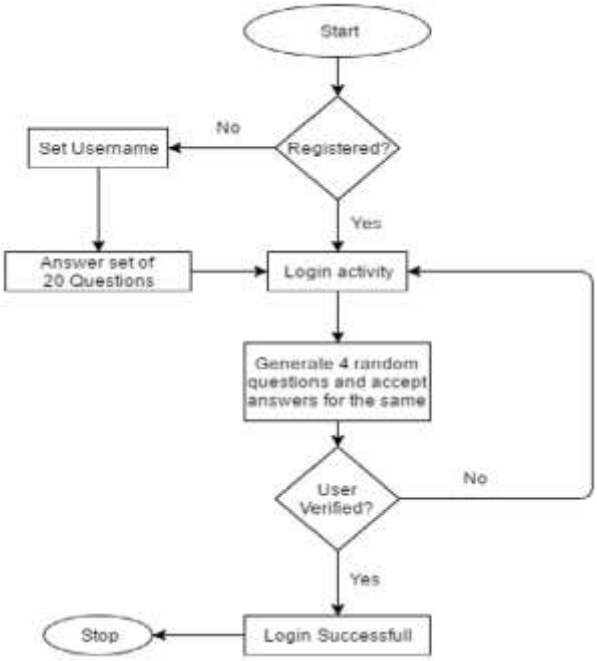
To developed a prototype on Android smart phones, and evaluate the security of the secret questions by asking the acquaintance/stranger who participate in our user study to guess the answers with and without the help of online tools meanwhile we observe the questions reliability by asking participants to answer their own questions. Here we are define the problem is that the device won't be able to recognize whether the voice is spoken by a person the voice is disguised by someone else. Other point was covered that since the device cannot recognize the person, hence a recording of the person's voice can also bypass the system [4]. Finally, a person with similar voice pattern can easily bypass the system which uses voice recognition.

III. METHODOLOGY:



We can say that the security of the current system is not reliable and secure. And since this technology is one of the most promising upcoming technology which interacts with the user's data. Hence, Security should be strong and reliable. The main aim is to enhance the security of PDAs so that they can be use anywhere without the risk of letting nefarious people know the passwords while using it in public place, and keeping the system more secure as well as the user's data. From the limitations of the existing system, we know that there is a need of adding another layer of authentication so as to keep system more secure.

System login Flow chart:



1. SYSTEM MODULES:

- Verbal Password
- Digital assistants

In this module we have three sub modules:

- Personal
- Personal Authentication
- Monitor Phone

2. TECHNOLOGY USED:

MD5 (MESSAGE DIGEST) HASH ALGORITHM:

The MD5 hashing algorithm is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message. The MD5 hash function was originally designed for use as a secure cryptographic hash algorithm for authenticating digital signatures. MD5 has been deprecated for uses other than as a non-

cryptographic checksum to verify data integrity and detect unintentional data corruption. Although originally designed as a cryptographic message authentication code algorithm for use on the internet, MD5 hashing is no longer considered reliable for use as a cryptographic checksum because researchers have demonstrated techniques capable of easily generating MD5 collisions on commercial off-the-shelf computers. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit 'fingerprint' or 'message digest' of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be 'compressed' in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

The IETF suggests MD5 hashing can still be used for integrity protection, noting "Where the MD5 checksum is used in line with the protocol solely to protect against errors, an MD5 checksum is still an acceptable use." However, it added that "any application and protocol that employs MD5 for any purpose needs to clearly state the expected security services from their use of MD5."

3. SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENT:

- Android Smart Phone
- USB cable

SOFTWARE REQUIREMENT:

Software	: ANDROID STUDIO
Language	: Java
Web Technologies	: PHP
Database	: My SQL
Java Version	: J2SDK1.8
Server	: Wimp Server

Application:

- Online social network
- Online banking
- Web application

IV. Conclusion:

The need for the transformation from text based data feeding to voice based data feeding is the dawn of a new technology which will require security and authentication over voice. The proposed system very well determines all possible loopholes that could be generated with this transformation and alleviates the same using challenge response and self-learning mechanisms. Also, the fact that voice recognition is still in its infant stage, is very well adopted by the system as it aims to act like a second level of authentication ensuring that unauthorized breach never occur even when voice recognition fails.

V. FUTURE SCOPE:

In future work, we will extend the challenge response protocol to further demonstrate the abilities of this protocol with voice. We will look into expanding the challenge response protocol, improving security and robustness, by examining the types of questions than can be asked. One of the ways this will be accomplished is by mixing the text-dependent work done so far with text independent modeling; allowing us to extend beyond basic words and phrases. Adding speech detection to the system also increases the number of bits. If, during the verification process, the system is also able to determine what the spoken phrase is, more bits would be added.

VI. REFERENCES

[1] Aaron Gala, Defang Mistry " **Verbal Authentication for Personal Digital Assistants**" in 2017 IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 09-13

[2] Sarabjeet Singh, Yamini M **"Voice Based Login Authentication For Linux"** in 2013 International Conference on Recent Trends in Information Technology (ICRTIT).

[3] R.C. Johnsona,b, Walter J. Scheirera,c and Terrance E. Boulta,b "Secure voice based authentication for mobile devices: Vaulted Voice Verification" in 2012.

[4] Dong-Ju Kim, Kwang-Woo Chung, and Kwang-Seok Hong **"Person Authentication using Face, Teeth and Voice Modalities for Mobile Device Security"** IEEE transactions on Consumer Electronics, Vol 56, No.4 November 2010

[5] Jean-François Bonastre, Frédéric Bimbot, Louis-Jean Boë, Joseph P. Campbell, Douglas A. Reynolds, Ivan Magrin-Chagnolleau **"Person Authentication by Voice: A Need for Caution"** in EUROSPEECH 2003: GENEVA.

[6] Qi Li, Biing-Hwang Juang, Qiru Zhou and Chin-Hui **Lee "Automatic Verbal Information Verification for User Authentication"** in IEEE transactions on speech and audio processing, vol. 8, no. 5, September 2000.