# A NOVEL WAY OF INTEGRATING VOICE RECOGNITION AND ONE TIME PASSWORDS TO PREVENT PASSWORD PHISHING ATTACKS

K Marimuthu, D Ganesh Gopal, Harshita Mehta and Aditya Rajan, P Boominathan

School of Computing Science & Engineering, VIT University, Vellore-632014, India

## *ABSTRACT*

*Phishing is a threat to all users of the internet who intend to use the web for secure transactions. In the recent years the number of phishing attacks have increased drastically especially since the advent of e-commerce, net banking and other services that have an emphasis on security. Phishing is characterized as any malicious attack aided by a spoofed webpage to encourage users to input their security details. Phishing is largely done to retrieve passwords and security details of unsuspecting users. This paper details a new and more secure way to counteract the method of phishing.*

## *KEYWORDS*

*Anti phishing, One Time Password (OTP), Authentication, IM service, Voice/Speaker Recognition, Cloud Computing.*

## 1. INTRODUCTION

A one-time password (OTP) is a password that is valid for only one login session or transaction. It overcomes a lot of shortcomings of static passwords which can be cracked, guessed or stolen. Also it is a hassle for a user to remember so many passwords. Companies are turning towards new methods of authentication like one time passwords. But, one time passwords are not impregnable to attack. As more and more websites employ this method and attackers are coming up with sophisticated ways to compromise such systems, we propose a better system consisting of sending an OTP only after voice recognition of the user and storing all the data on the cloud. This makes the system more secure as duplicating a voice is very difficult, making it almost impossible for an attacker to harm the system. In this section we discuss the existing phishing and anti -phishing techniques and also the methodologies that we use in our solution.

### 1.1 EXISTING PHISHING METHODS

1. Domain Spoofing : Phishers may use similarly spelt website names as well as names that look similar to the actual domain to fool unsuspecting users into providing confidential. information e.g.: Substituting lower case letter 'l' for capital letter 'i' since they look similar.
2. URL Modifying: Using the '@' symbol lets phishers redirect traffic to their own url as web browsers truncate all character before the '@' symbol. For example google.com@192.168.1.1 will redirect to 192.168.1.1 without regarding the google.com URL.
3. Website similarities can also be used to trick users into believing that the phishing site is actually the original. This can be facilitated via image and font similarities as well as general layout similarities. Also positioning of text boxes can trick users who do not pay much attention to detail. [1]

## 1.2 CURRENT ANTI PHISHING TECHNIQUES

- Content Filtering: It consists of web filtering for scanning websites and email filtering to check for spam and other objectionable content using methods such as Bayesian Additive Regression Trees (BART) or Support Vector Machines (SVM) [2]. The major drawback of this method is that the web filter will block the wrong sites on a general basis for simply containing an objectionable word [4].
- Black Listing: It is an access control mechanism which identifies phishing sites and denies access to them. White list includes elements which are allowed access and grey list includes elements that are temporarily blocked until an additional action is performed [2]. The disadvantage is the time it takes to identify a phishing site. The phishing sites these days are hosted on the internet for a very short duration and try to trap as many users as possible. The blacklisting process cannot be done fast enough to be successful in blocking attacks [4].
- Symptom based prevention: Symptom-based prevention analyses the content of each Web page the user visits and generates phishing alerts according to the type and number of symptoms detected [2]. Spoofguard[10] is a symptom based plugin solution. But a hacker can gain access to a user's computer disable the plugin making it prone to phishing.
- Domain binding: - It is a client's browser based techniques where sensitive information (e.g. name, password) is bound to particular domains [2]. It warns the user when he visits a domain to which user credential is not bound. Phishers can acquire certificates for domains they own and certification authorities can make mistakes.

## 1.3 THE CLOUD MODEL

The cloud is a computing hardware machine or a group of them known as a server connected through a communication network like internet, Local Area Network [LAN], Wide Area Network [WAN] or intranet. Any user who has permission to access the server can use it for storing of data, running an application or any other computational task. It is mainly of 3 types:

Software as a Service (SaaS): The cloud providers manage the infrastructure and platform while the client has access to application software and databases. It has more security risks.

Platform as a Service (PaaS): It is a shared environment where the application developers run their software solutions on a cloud platform and the cloud provider provides the platform i.e. web server, database, programming language execution environment and operating system. Eg. Windows Azure.

Infrastructure as a Service(IaaS): Consumer controls processing, networks, storage and other fundamental computing resources and provider controls operating system and deployed application. E.g. Amazon Elastic Compute Cloud [7].

This solution will use cloud as PaaS. This proves to be extremely useful as in this field of computing, security is of the highest importance. The storing of voice passwords as well as generation of the OTP on the cloud allows them to be totally separated from the user's device or website. But it is important to ensure that the cloud provider you choose also offers physical colocation services. Then if your platform in the cloud needs to speak to applications on other platforms, this flexibility of physical colocation will work to ensure successful interoperation.

### 1.4 VOICE BIOMETRIC

Voice biometric is of two types :Text dependent: the password is same for registration and login or the user can repeat a randomly generated phrase.Text independent: Based upon whatever user says [8].Companies like VoiceTrust [9] and Nuance have created voice recognition softwares. [10].The voice password system consists of web applications, processing server and the database system as shown in Fig.1. [10].

The processing server hosts the web applications and stores data in the database. Speaker recognition analyses the frequency as well as attributes of voice signal like pitch, loudness, duration and dynamics. Then voice recording is separated into windows of equal length called as feature extraction. Following which is the pattern matching based upon Hidden Markov Models which take into account the underlying variations and temporal changes of the acoustic pattern. It involves the comparison of the speaker models with the extracted frames.

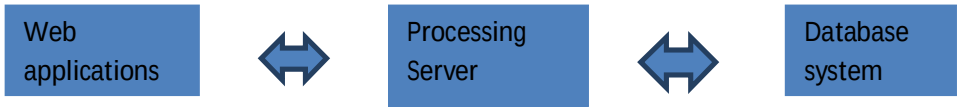



Fig.1. Voice Password System

### 1.5 DRAWBACKS OF THE CURRENT SYSTEM WITH ONE TIME PASSWORDS

1. The existing system can be compromised by attacks on the 3 components: user's website account, the websites IM account and the users IM account. A lot of advanced phishing techniques have come up like tab napping, spear phishing techniques like bouncer list [5].
2. If the attacker knows the users web account through clone phishing, link manipulation [6] etc. and is able to phish the IM account then the system is compromised. . Alternatively, if user is tricked into logging into a fake website, he will be asked to input his Web account name. Then, the fake site will display an OTP input page and wait for user to input the correct one-time password. At this stage, Attacker sends an authentication message to user's IM account using either the website's IM account or the IM account of one of user's friends and would successfully phish the OTP [3].
3. An attacker can launch a Man In The Middle attack on a user and a website and can monitor all messages sent to or received by the user. If an OTP is discovered, the system becomes vulnerable to attack.
4. Phishing of the IM service,the phisher can phish the IM service by either inserting a custom IM client into the users personal computer or trick the user into logging into a fake website.[3]

## 2. THE PROPOSED SOLUTION

The proposed solution consists of two processes: registration process and login process. There are namely 5 parties: The user, the website, the IM service, cloud provider and phisher. We assume that website has joined one or more IM services and also has a registered cloud provider (e.g. VM Ware, Microsoft, Google Cloud Platform, etc.) for storing user data. The user should have access to secure internet connection especially if OTP is sent via email. The website can also choose other IM services like SMS. The general system architecture is shown in Fig.2.

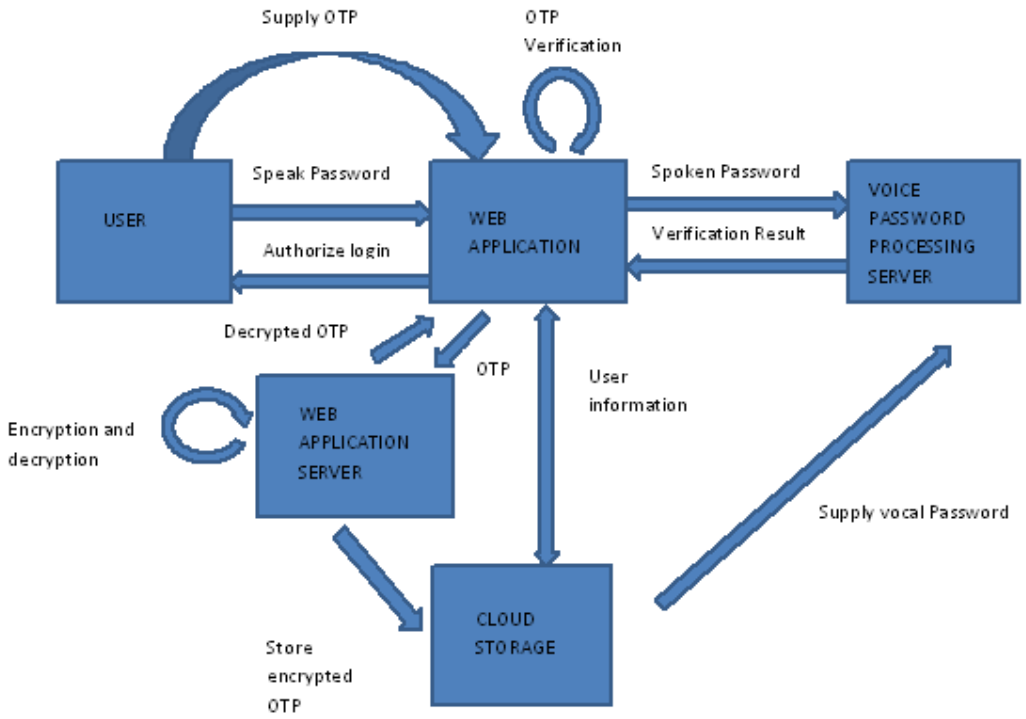



Fig.2. System Architecture

## 2.1 THE REGISTRATION PROCESS

This process involves the user to supply their personal details like name, email, phone number, etc. Our goal is to eliminate the use of static passwords and username.

The steps as shown in Fig.3.are as follows:

1. The user initiates signup. He/she must supply all the details. A CAPTCHA test can also be included to distinguish humans and computers. Then the user clicks save.
2. As soon as the user does this a unique username is generated using a random function.
3. The unique username is displayed and the user is asked to supply a voice password.
4. The voice password is confirmed twice or thrice depending upon the voice recognition software being used.
5. The voice password or the voice print is stored as a media file on the cloud along with the other information.
6. A confirmation message is sent to the user through the registered IM service.

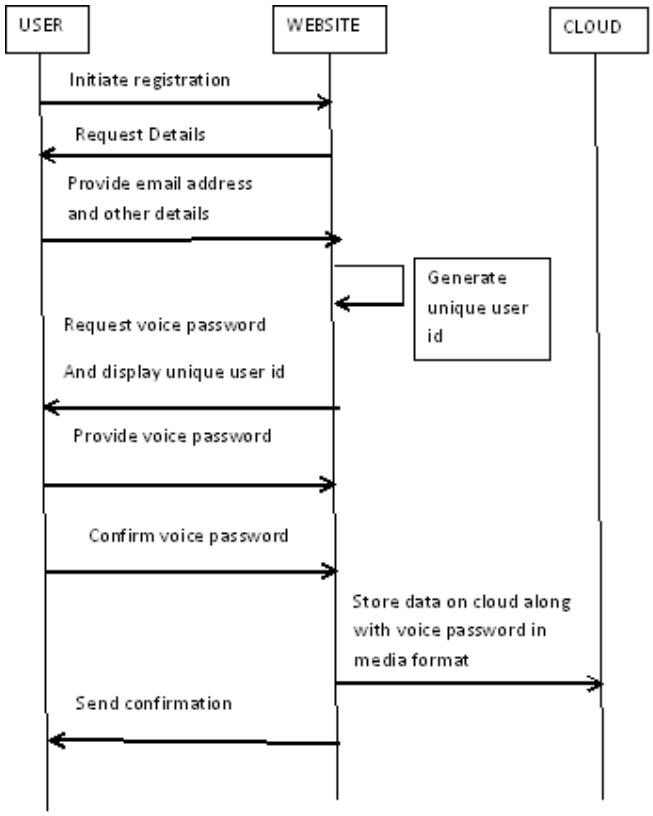



Fig.3. Registration Process

## 2.2 THE LOGIN PROCESS

The following steps are followed during the login process as shown in Fig.4.:

1. When the user initiates login he must first supply the unique User Id.
2. As soon as the User Id is verified a random OTP is generated using the Time based One Time password algorithm [11] and is stored on the cloud under the OTP detail.
3. This OTP is then sent using the secure IM service registered by the user.
4. The OTP will be valid for a fixed amount of time.
5. Once the user supplies the OTP, the OTP server automatically decrypts the stored OTP and it's compared to the input OTP.
6. After the OTP is verified the user is requested to speak the voice password. This password is compared to the voice print stored on the cloud.
7. If they match the user can successfully login.

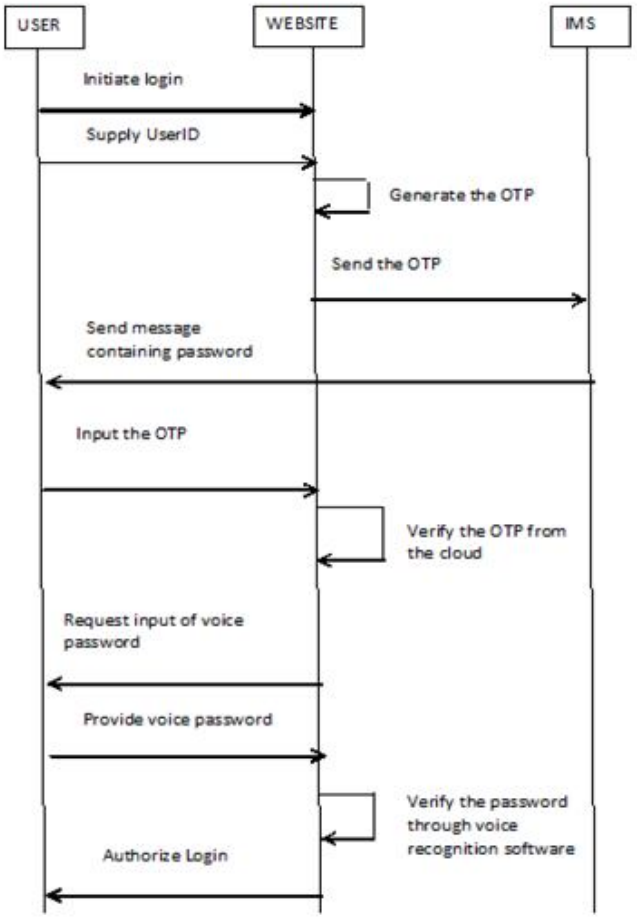


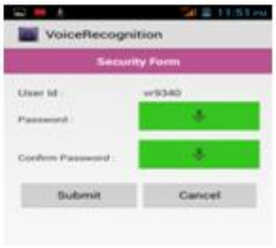

Fig.4. Login Process

## 3. IMPLEMENTATION

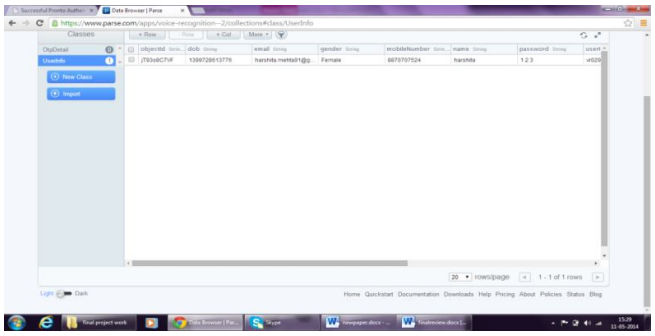
This section will give a demonstration of the processes involved in the proposed solution.

1. The user initiates login and supplies details.

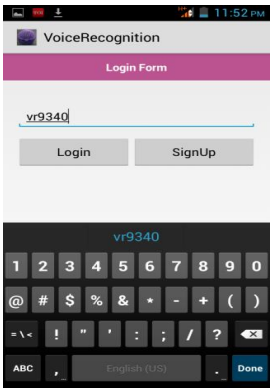
2. Unique user Id is generated and user is asked to supply voice password.



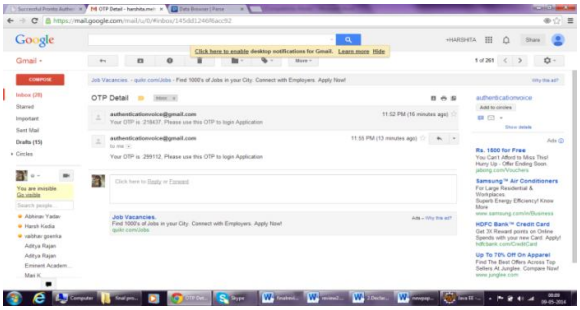

3. This data is stored on the cloud along with voice password. For this demonstration cloud service parse.com is used [16].



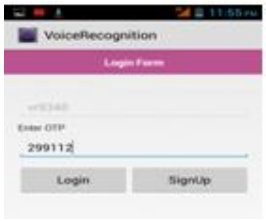
4. The user supplies username.




5. The OTP is sent via an IMS.



6. The user will input OTP.




7. The user will then input the voice password.


8. The user successfully logs in.


# 4. SECURITY ANALYSIS

## 4.1 Text Independent Voice Biometric

The user speaks the same password as supplied by him during the registration. This is better than the text independent speaker recognition because text independent requires more training and testing utterances to achieve good performance. This solution will fail for mute people and people with vocal problems. Voice is a unique combination of behavioural and physiological factors and is better than fingerprint. Also it does not require a camera like in case of retina scan. But the only issue with voice recognition is the system. The setup for voice recognition needs to be robust as voice quality depends upon environment and also is vulnerable to mispronunciations. Also there is the problem of spoofing where a person tries to imitate the voice but this system has an extra layer of security through the OTP. Also the voice print is not stored anywhere in the system or mobile database of the user or the website or the database of the voice recognition system.

## 4.2 The man-in-the-middle attack

The man in the middle attack is when a malicious attacker intercepts the messages between two devices. The attacker might tries to discover the OTP but it won't be possible as it is sent through a secure channel. Also if the OTP is discovered it is useless without the unique username and the voice password. Also the OTP is valid for a short duration and the next OTP

can't be predicted because it is based on the Time based One Time password algorithm[11] which is highly randomized.

### 4.3 Improving Cloud Security

As most of the critical information is stored on the cloud it might become the target of attack. Many companies have come up with exceedingly secure ways for cloud security. For example, Vormetric [12] works with both cloud providers and companies to protect the data. They protect both data and encryption keys. Another example is the VMware vCloud Infrastructure software [13] that tracks applications as they move through the cloud ensuring a correct firewall configuration. Thus, a number of ways have come up to improve cloud security.

### 4.4 Other advantages

This solution is not compromised even in case of device theft. Even if the user logs in an untrusted environment it will be exceedingly difficult for the attacker to compromise the whole system with multi levels of authentication. The attacker can also not make a user logon to a fake website as the attacker has no information about the data stored on the cloud which includes the voice print.

### 4.5 Comparison with other OTP mechanisms

| PARAMETERS | PROPOSED SOLUTION | ONLY ONE TIME PASSWORDS[3] | TOTP BASED ONE TIME PASSWORDS[11] | PUBLIC KEY ENCRYPTION FOR OTP TRANSMISSION[14] [15] |
|---|---|---|---|---|
| Man-in-the-middle attack | Not possible because: unique username voice biometric cloud storage | Very much plausible | Very slight possibility but if happens the next password is impossible to know Also the password is valid for only 30 seconds | Very slight possibility |
| Impersonation | Not possible Voice print is unique to an individual | Possible if IMS service is compromised | Not possible | Possible Even if user's private keys are not available a successful attack on certification authority will allow an adversary to impersonate anyone by using public key certificate from compromised authority to bind a key of adversary's choice to name of another user. |
| Website's database | Highly improbable | Very much possible | System can be compromised | System can be compromised. |

| | | | | |
|---|---|---|---|---|
| compromised | because data is stored on cloud and is also encrypted | | | |
| Overhead | NO<br>Speed is fast | NO<br>Speed is fast | NO<br>Speed is fast | Significant overhead on local and remote application programs<br>Very slow speed |
| IM service compromised | No effect as voice recognition provides additional security | System compromised | System can be compromised in spite of the password being valid for 30s | System Compromised |

## 5. CONCLUSION

The use of One Time Passwords, Cloud Computing and Speaker Recognition leads to increased security. This is due to the multiple levels of access that a hacker has to breach. The system proposed is stronger to the existing system hence. The one-time password generated by a secure hashing method, the storage of information on the cloud and not on the user's device , the system of user and website and the additional voice password increases overall effectiveness. This system is highly secure and robust. Future Work will include coming up with even more efficient softwares of voice recognition which work in any environment irrespective of the noise.

## REFERENCES


[1] Phishing Exposed, Lance James
[2] Hicham Tout, William Hafner "Phishpin: An identity-based anti-phishing approach" in proceedings of international conference on computational science and engineering, Vancouver, BC, pages 347-352, 2009
[3] Using one-time passwords to prevent password phishing attacks, Chun-Ying Huang , Shang-PinMa , Kuan-TaChen, Elsevier Journal of Network and Computer Applications 34 (2011) 1292–1301
[4] Phishing and Countermeasures:Understanding the Increasing Problem of Electronic Identity Theft, Markus Jakobsson, Steven Myers,John Wiley & Sons
[5] www.phishing.org
[6] Hacking: The Art of Exploitation, 2nd Edition , John Erickson
[7] Cloud Computing Explained, John Roton, 2013 edition
[8] http://www.biometric-solutions.com/solutions/index.php?story=speaker_recognition
[9] http://www.voicetrust.de/en
[10] http://www.nuance.com/ucmct/groups/imaging/@web-enus/documents/collateral/nucc1021vocalpasswordv9proddes.pdf
[11] http://tools.ietf.org/html/rfc6238
[12] http://www.vormetric.com/sites/default/files/wp-data-security-in-the-cloud.pdf
[13] Whitepaper: file:///C:/Users/USER/Downloads/Whitepaper-VMware%20Bluelock%20Security%20In%20The%20Hybrid%20Cloud.pdf
[14] One-Time-Password-Authenticated Key Exchange, Kenneth G. Paterson, Douglas Stebila, Information Security and Privacy Lecture Notes in Computer Science Volume 6168, 2010, pp 264-281, Springer Journals
[15] Simple Password-Based Encrypted Key Exchange Protocols, Michel Abdalla, David Pointcheval
[16] https://www.parse.com