Two Way Mobile Authentication Security Mechanisms for an Enterprise System

Ayangbekun Oluwafemi J[1]., Olowookere A. Sunday[2], Shoewu Oluwagbemiga[3]
[1]*Department of Information Technology, Crescent University Abeokuta, Ogun State. Nigeria.*
[2] *Department of Computer Science, Oyo State College of Agriculture, Igbo Ora. Oyo State, Nigeria.*
[3]*Department of Electronic and Computer Engineering, Lagos State University, Epe Campus*

ABSTRACT : *Over a decade and more importantly since the advent of Internet technology, security issue has become a thing of great necessity to protect an enterprise data. This has culminated as a result of an increase in cybercrime by hackers thereby bridging the confidentiality and data integrity gap of an enterprise. Therefore to prevent an unauthorized user access by the intruders/hackers into a personalized data or information, there is need for a stronger mode of user's authentication that goes beyond the usual ID and password authentication mode which is regarded as the One-way authentication system. This paper however illustrates and describes a two-way mobile authentication factor as an improvement over the traditional one way authentication factor. Our proposed system requires both the Web and a GPRS connection for its online authentication via the designed web based interface and gets a randomly generated OTP via short message service on his mobile phone, which he must then type-in to be granted access to the system and access the available resources.*

Keywords - *Authentication, Biometric, Code, Enterprise, Mobile.*

I. INTRODUCTION

Authentication is the act of confirming the truth of an attribute of a datum or entity. It involves confirming the identity of a person or software program. By definition authentication means using one or more mechanisms to prove that the persons is who he claims to be. [1]. However authentication mechanism requires both a web and a GPRS. Roberto Di Pietro [2] one of these solutions for this issue is the two factors authentication technique and implementation issues. The need for better and more secure systems has given rise to the concept of the two factor authentication system. In this new system, first factor is just usual password that everyone creates while registering or creating an account. A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to resource (example: an access code is a type of password). However the password should be kept secret from those not allowed access.

In modern times, user's names and passwords are commonly used by people during a login process that controls access to protect computer operating system, mobiles phone, cable TV decoders, and automated teller machines (ATMs), etc. A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving e-mail from servers, accessing programs, databases, networks, web sites, and even reading the morning newspaper online. One of the major areas of security improvement is the way in which authentication of users is carried out. Even though many organization still rely on static ID and password authentication system, this method is getting old and there is a requirement for a better way of authentication which is required. One of the solutions for issue is the two factor authentication technique as a fundamental security function. This thesis explores the two factor authentication technique and implantation issues, which is regarded as a process or technology in which both entities in a communications link authenticate each other.

Based on the online security challenges being orchestrated by hackers who gains unauthorized access into an enterprise data, the one way authorization system access is being considered not effective enough to combat this menace of data insecurity. Therefore, the two way mobile authentication system came into being to provide more security features through the use of a personified/personalise data requirements to gain access for stronger and a more robust authentication.

In existence, the three major factors for authentication includes: what you know (e.g. passwords, PIN's), what you have (e.g. smart cards or tokens), and what you are (e.g. figure prints, face recognition, biometrics, etc). In the context of this paper, the proposed systems which requires the users to supply his/her one time password (OTP) for login as well as the second password/data which the user in question receives as an SMS on a registered number in the developed application to gain access into the enterprise system. This however makes the system much more stronger and secure than the traditionally Implemented one factor authentication system.

One of the examples of two factor authentication includes withdrawing money from an ATM machine. When someone wants to draw money from the ATM, first he\she has to input his\her ATM card i.e. what you have and again he\she has to enter the pin number i.e. what you know in order to access his\her account. Recent work has been done in trying alternative factors such as a fourth factor, e.g. somebody you know, which is based on the notion of vouching. Only recently, two-factor authentication systems based on mobile devices have started to gather some interest within the research community. An authentication mechanism presented here requires both a Web and a GPRS connection. The end user enters use rid/password details using a web-based interface and gets an OTP (One Time Password) via short message service on his mobile phone, which he must then type in to be granted access to the system. The General Packet Radio Service (GPRS) connection is not convenient for the user since it can be very costly and network quality of service (including availability of network coverage) is not always satisfactory. In addition, security of the scheme relies on information (image) related to the user, but the underlying rationale needs to be expanded with further arguments.

II. LITERATURE REVIEW

Authentication mechanisms involves the procedural steps require by an authorized user to gain access to some data or grant access to certain resources. In this respect, validation of user's requirements and identity is highly crucial. This can be carried out via different mechanisms such as Username and Password, PIN, tokens, access card and any means of pattern recognition features (such as finger prints, face recognition, biometrics to mention a few). However, the two way factors authentication is a more secure [1] means of authentication than the one factor authentication because it combines both what the user knows (such as password) and the biological identification features (pattern recognition – biometrics features like Fingerprints, retina recognition etc.) inherent in an individual.

2-Way Mobile Authentication is all about an Innovative authentication system that provides access to Web-based resources by using a two-way user authentication through the existing personal mobile phones. It is used to solve the security flaws of the web password, and a code which they get only during authentication (a one-time password OTP sent to their mobile phone) before they are permitted to access a secured web based Internet and Intranet, by involving the users to authenticate themselves using their personal mobile phones. The registration of the users has to be done in a secured manner before resource [7]. With 2-Way Mobile Authentication System, we can positively identify users and deliver services easily and in a most secured way to users, without having the need of an additional security system. End users can have the advantages of a very simple process that omits the need to remember multiple passwords. The main reason for moving from one-way to two-way authentication is that the 2-way mobile authentication performs better than the other existing systems in terms of cost, complexity and protection [7]. It is widely used and supported by the largest number of applications Technology easily understood by users. 2-way authentication is making up of OTP generation software/hardware or access to a secondary channel for OTP transmission and password.

The main benefits of 2-way mobile authentication is that we can positively identify users and deliver services easily and in a most secured way to users (Table 1), without having the need of an additional security system. It is also designed to provide security to Web-based Internet and Intranet applications, and requires users to authenticate themselves with two unique criterions - a username and a transaction.

Table 1: Differences between One and Two way Authentications

One way Authentication	Two wayAuthentication
Is the authentication of only one end of a communication session.	Is the process or technology in which both entities in a communication links authenticate each other.
Allows the clients to verify the identity of the server it is communicating with only.	Allows both the clients and the server to verify one another.
Single protocol exchange to authenticate one party to another.	Double protocol exchange, which enables both parties to authenticate each other.

In this system an authentication mechanism is presented and it requires both the Web and a GPRS connection. The end user enters user ID (identity)/password details using a web-based interface and gets an OTP via short message service on his mobile phone, which he must then type in to be granted access to the system. The General Packet Radio Service (GPRS) connection is not convenient for the user since it can be very costly and network quality of service (including availability of network coverage) is not always satisfactory. In addition, security of the scheme relies on information (image) related to the user, but the underlying rationale needs to be expanded with further arguments [2].

In this phase, a stronger authentication mechanism is developed based on information stored in a Subscriber Identity Module (SIM) card

and the Authentication Centre of the subscriber's carrier. One drawback of this approach is the necessity for the financial service provider to enter into a prior agreement with the network carrier. A biometric authentication is the advanced form of authentication. A biometric authentication is nothing but it scans the user's characteristics such as finger print and eye retina and stores in the form of a string. When the user tries to authenticate it matches with the stored data and then gives access when a commonality is achieved and when the user has gained access he can enter the password to view the required information [3].

A better, more secure way of authentication is the so called "two-factor" or "strong authentication" based on one time passwords, instead of authenticating with a simple password. Strong authentication solutions using two identification factors require often an additional device, which could be inconvenient for the user and costly for the service providers. To avoid the usage of additional device, the mobile phone is used to receive the onetime password [4]. Two-factor authentication provides shielding for Enterprise and their customers from MITM attacks. The two-factor authentication model uses an online password and an additional form of authentication (such as using one time password) for online security [5]. Mobile Id offers a strong two way authentication by authenticating the user to the service and service to the user. The mobile id works is such a way that the user is required to send the code generated by the application after which the Mobile id generates a code to identify the user with the service.

One of the method used in generation of OTP (One Time Passwords) is by using a mathematical algorithm to generate a new password based on the previously generated password (i.e., OTP (One Time Passwords) are, effectively a chain and must be used in a predefined order). This is not secure because once the hacker finds what sequence of passwords is using by the user; he can easily trace out the future OTP (One Time Passwords). The cheapest way would be generating a One-time password and then delivering it on a piece of paper which is already known by someone who generates the OTPs on a device. The reason for this is these systems avoids the costs of SMS messaging .Even though delivering the OTPS by this way is cheap, it is not feasible because of the time to deliver the password to the user is too long [6]

Dynamic password (namely, One-Time-Password) technology is a sequence password system and is the only password system proved non-decrypted in theory [2[. The 2 Way mobile authentication system could not replace the existing authentication system, but instead serves as an added layer of security that protects and enriches the existing authentication system, either software or hardware [6].

III. TYPES OF AUTHENTICATION

There exist four (4) major types of authentication

- Windows Authentication
- Forms Authentication
- Passport Authentication
  Anonymous Access

IV. TWO WAY MOBILE AUTHENTICATION ARCHITECURE

This Two-Way Mobile Authentication employs the use of mobile phones randomly generating certain codes to an individual as another way of authentication before gaining access to Web-based resources in a more secure manner.

It is designed to provide security to Web-based Internet and Intranet applications, and requires users to authenticate themselves with two unique criterion - a username and password, and a code which they get only during authentication (a one-time password OTP sent to their mobile phone) before they are permitted to access a secured web resource [7].

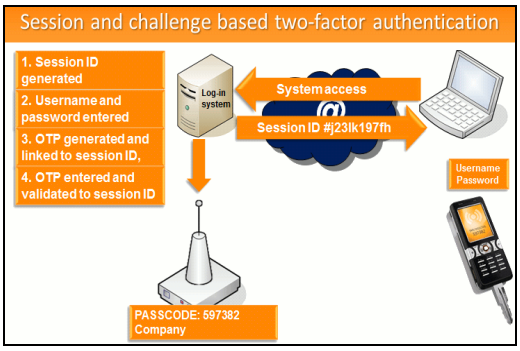

Figure 1: Two way Mobile Architecture

Fig. 1 explains how the authentication of the system is being carried out. When the session ID is being generated i.e. filling the online application form, the username and password which is being generated are entered. This takes us to the phase of SMS authentication where the OTP is being created and linked to validate the session i.e. the Personal Control Area.

V. HOME SCREEN DESIGN

The homepage (Fig. 2) of the authentication system is the main point of this research. The authentication is required to gain access into one's personal account, thereby ensuring security of individual users account details.

Figure 2: Homepage

VI. BACKEND DESIGN

Database can be maintained by defining a set of proactive tasks that a DBA (Database Administrator) needs to perform on a periodic basis to help ensure that their databases perform optimally and maintain high availability. The database for the log-in procedural steps for the authentication system is shown below (Fig. 3).

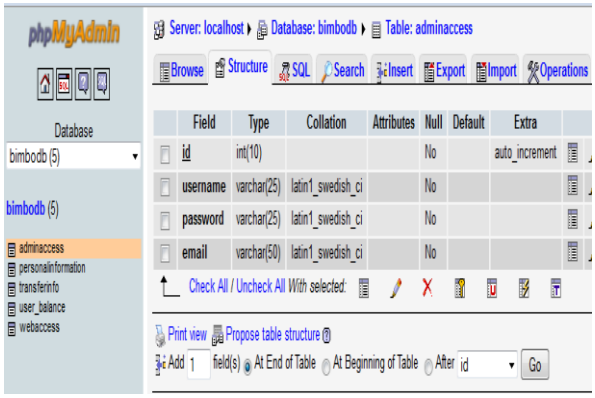

Figure 3: Log-in Database

VII. SYSTEM ACTIVATION AND AUTHENTICATION

After the registration, an individual account will be automatically created and ready for use (Fig. 4).

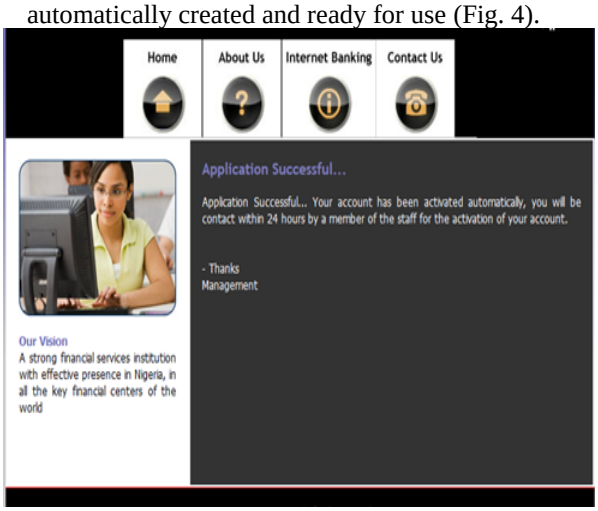

Figure 4: Users Activation

However, Authentication takes two forms.

- The user is expected to log-in on the logging-in panel at the bottom right of the homepage (Fig. 2) with their username and password based on the criteria supplied during registration phase. If the user login is correct, an SMS code is sent to the users' mobile number (Fig. 5).

Figure 5: Mobile Phone

- User is redirected to the second authentication phase where user enters the generated mobile sms code is logged - in for authentication (Fig. 6).

Figure 6: SMS Authentication

Having succeeded in the two stages, the user will be directed to his personal area where he can perform any transactions.

VIII. CONCLUSION

This research aims to study and implement the two way mobile authentication for enterprise system and analyzing its advantages over the one way authentication system. The research was initially examined and analyzes the controversial usual traditional way of authentication which

involves the use of username and Password/Pin to gain access to online resources. The analysis was concluded and states the urgent need to introduce the two way authentication system as a more secure and reliable mode of authentication for an enterprise system.

The implementation phase then follow by designing a web based application using PHP incorporated by an object oriented programming language for the design phase. The mobile phase was designed using JAVA programming language based on its robustness and its ability to run on a web platform. The One Time Password (OTP) was sent to the GSM user through a SMS gateway provider required for an authentication.

Three Factor/Biometric-based authentication techniques also exists and its more convenient, safe and reliable. This system is pattern recognition system in which a person is recognized based on features derived from specific psychological or behavioral characteristics that the person possesses, which are difficult to be guess or stolen.

REFERENCES

[1] Aloul F, Zahidi S, El-Hajj W. (2006): *Two Factor Authentication Using Mobile Phones, IEEE/ACS International Conference on Computer Systems and Applications.*

[2] Roberto Di Pietro, Gianluigi Me, Maurizio A.Strangio . *A Two –Factor Mobile Authentication Scheme for Secure Financial Transactions. International Conference on Mobile Business 2005.*

[3] H.B Kekre,V.A Bharadi, (2009): *International Journal of Intelligent Information Technology Application,2(6):*279-285

[4] Do Van Thanh Jorstad , Do Van Thuan and I. Jonvik (2009): *Strong Authentication with Mobile Phone as Security Token, Mobile Adhoc and Sensor Systems, IEEE 6th International Conference.*

[5] Aloul F. etal, (2006): *Authentication means using one or more mechanisms to prove that the person is who he claims to be.*

[6] Harris, J.A. (2002): *A One Time Password Scheme .International conference on Parallel Processing Workshops, Proceedings.*

[7] Harish Dinne and Karthik Mandava (June 2010): *Two way Authentication System",Blenkinge Institute of Technology, Sweden.*