Password Authentication System using New Intense Secure Algorithm in Mobile and Server in Two way Communications

B.Shanmuga Sundari (AP / IT)
Dept.of information Technology
PET Engineering College (Vallioor)
Tirunelveli, TamilNadu,India (627117)

G.Anusooya Devi (Author)
Dept. of information Technology
PET Engineering College (Vallioor)
Tirunelveli, Tamil Nadu, India (627117)

S.Shahina (Author)
Dept. of information Technology
PET Engineering College(Vallioor)
Tirunelveli, Tamil Nadu, India (627117)

ABSTRACT
Authentication is the first line of defense against compromising confidentiality and integrity Traditional login password may not be used in every scenario its occurred lots of attacks. As an alternative PAST were introduced. In this paper introduce a framework of our proposed in two different verification code system were introduced.

***Keywords*—PAST**

Password Authentication System in Two ways communication

1. INTRODUCTION
Authentication is a process of determining whether a particular individual should be allowed to access a system or an application. According to Email, the unauthorized people easy to hack other user email Id. So its break in that ,so, commenced Password Authentication System Using New Intense Secure Algorithm in mobile and server in Two Way Communications (PAST),to resolve Security and Usability Limitation.

In this paper commenced, discrete verification codes. They are two types**. Lock** and Release verification codes. **Lock code** is used to lock the system and **the release code** is used to release the system with the help of server

.
In this paper (PAST) is mainly technologically in user comfortable and satisfication.According to the application process, in Banking sectors and other relevant password security applications

Scope
- More protection
- High security
- Easy access to user

2. EXISTING SYSTEM
A password is a secret word, to admittance system. In every application needs some security. Security is the one and only to protect the schemes. So, it enhances Password, Now – a –day they are poles apart password initiated.

Username [ ]

Password [ ]

Login

Fig 1: basic structure of login the system

2.1 One way verification code
In present, the security enabling verification codes send through the SMS to the corresponding user mobile. These types of verification codes are generated in one way communication that is, the codes are received from the server then the user enter the codes in corresponding server application window.

2.1.1 Drawbacks
The verification codes are best approach to protect the applications or systems but in these one way verification codes lots of limitations are there. The users easy to access the codes but the codes enter the server application window. Here, we found SQL Injection attacks and user not contented.

2.2 SQL Injection
SQL injection is a technique often used to attack data driven applications This is done by including portions of SQL statements in an entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database (e.g., dump the database contents to the attacker). SQL injection is a code injection technique that exploits security vulnerability in an application's software. The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL commands are thus injected from an application form into the database of an application (like queries) to change the database content or dump the database information like credit card or passwords to the attacker. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

3. PROPOSED SYSTEM

Username [ ]

Password [ ]

Lock **Release** **Login**

Fig 2: basic structure of PAST application window

3.1 Two way communications

In this technique, why using two way communications

- **What is need of two way communications?**
- **Why we are using two way communications?**
- **What is the benefit of this technique?**

The server and clients access the verification codes through a SMS to a GSM cell phone .PAST typically provides a better security protection than static password

3.1.1 Mobile ID

Mobile id offers a strong two ways authentication by authenticating the user service and service to the user. *The* mobile ID works is such a way that the user is required to send codes generated by the application after which the mobile id generates codes to identify the user with the service.

3.1.2 SMS gateways

An SMS gateway is a telecommunications network faciity for sending or receiving Short Message Service (SMS) transmissions to or from a telecommunications network that supports SMS. Most messages are eventually routed into the mobile phone networks. Many SMS gateways support media conversion from email and other formats.

3.1.3 Vulnerability

PAST is mainly invoked by the recent vulnerabilities is mainly implemented in SQL injection.

1) How its works?

2) What are the challenges for hijackers?

In SQL database the data's are stored in specific functnalities.According to the email server the backend proccess of databases the corresponding users' *details* are warehoused

In current, hijackers are stolen the user details from the SQL databases.So, planned to breakout this attacks. In two way communications that is *server* to clients ,clients to server access the verification codes.The mobile access only main lead.If the corresponding user mobile service(SMS) codes only activated then the databases are shown the details.If it's not authorized user then the databases hidden the details.

4. REQUEST SYSTEM

The clients request to the server, then server check the client request and then the processing will be taken.

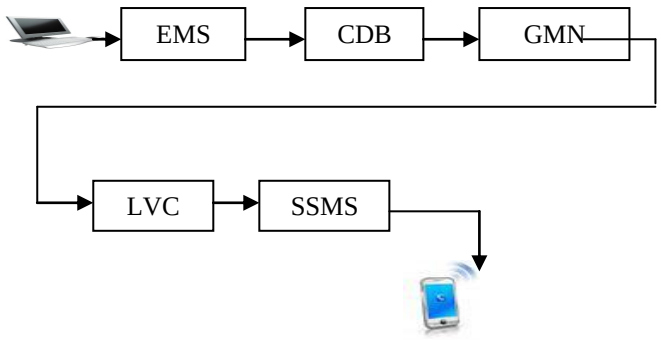

Fig 3: Request System process

EMS → ***Email Server***
CDB → ***Check Data Base***
GMN → ***Get Mobile Number***
LVC → ***Load Verification Codes***
SSMS → ***Send SMS through Mobile***

If the user chooses the lock folders, then the above process to be activated. The *analogous* email id is request to the email server. Then its goes to check the database and get the consistent user mobile number. Then, its moves to substantiation codes (lock Release) and send it through the SMS to the user mobile

5. RESPONSE SYSTEM

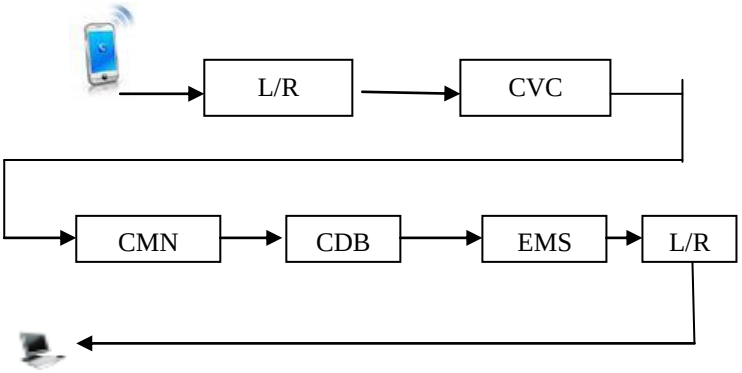

Fig 4: Response System process

L/R → ***Lock/Release***
CVC → ***Check Verification Code***
CMN → ***Check Mobile Number***
CDB → ***Check Data Base***
EMS → ***Email Server***
L/R → ***Lock /Release Condition***

If the user need to release/lock the email id means the above process to be activated. The user type the substantiation codes whether its lock/release send it *SMS* through the same server. Initially check the verification codes next to plaid the mobile number whether the

corresponding mobile number or not. Then the Email server plaid the status if it's correct means agreeing user request to be activated.

6. LOCK PROGRESS

Let assumes 200 types of codes is set to the program. For example (Lock code has ABCD and Release Code 1234) typically its swaps the orders and its monitoring the codes format .If lock statement is received then, it asks to the email server .The email server check the user details. Whether the user authorized means request system activated. According to the swap in corroborate code is loaded and, Clone with databases.

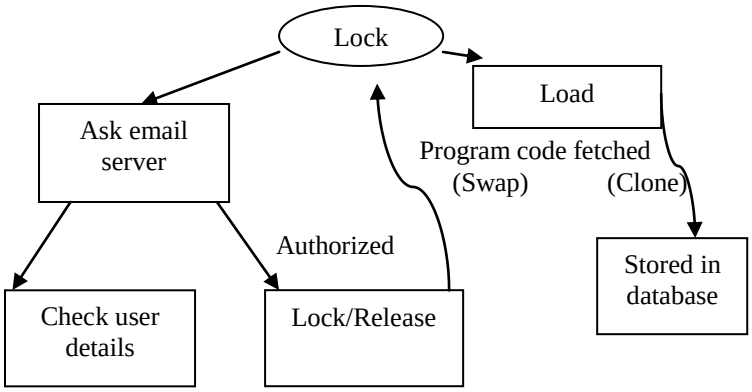

Fig 5: basic of lock progress

7. NOTIFICATION IN DATABASES

In databases verification codes are received then, it's shown a tick mark is obtained to the consistent data table. If it's not received then cross mark is obtained (that is no verification codes are loaded)

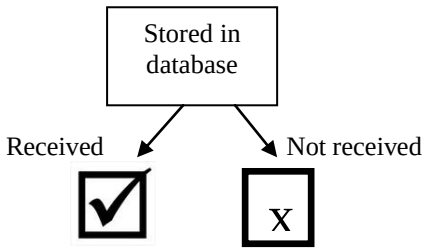

Fig 6.0: Status of substantiation Database

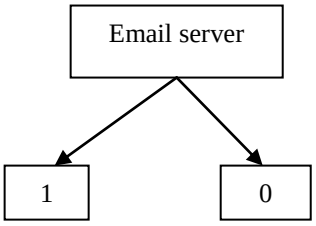

Fig 6.0.1 Status of request and response in email server

In email, typically provides verification codes to the user mobile if the user response then, the status of email server activated in 1 otherwise 0.

Table 1: Status of user response

Lock	Release	User Response	Status
abcdef	13675	abcdef	
cdefg	45899	45899	
ghijk	17789	17789	

In email server the user response status to be noticed for example (In first row, the lock code is abcdef and the release code is 13675 the user did response abcdef that is the user entered lock code so the status is red otherwise green)

8. TWO WAY COMMUNICATIONS

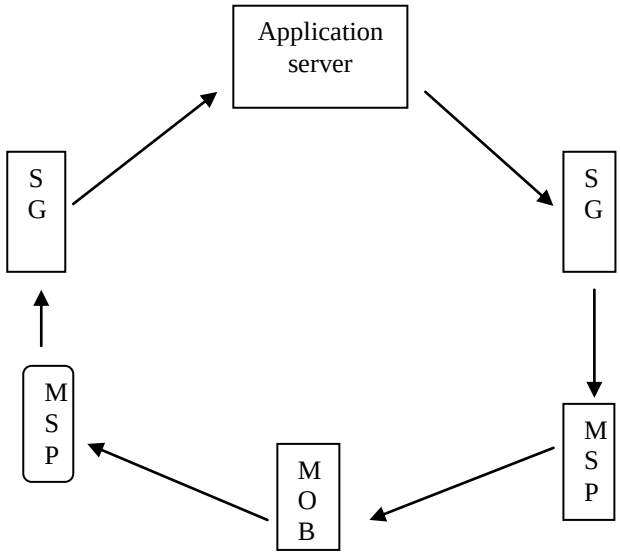

Fig 7: basic operation of two way communications

SG → ***SMS Gateway***
MSP → ***Mobile Service Provider***
MOB → ***Mobile***

Two-way SMS applications are more intricate than one-way.In two-way SMS applications, a user can initiate a conversation by sending messages, and then the application responds according to the user's commands. The life cycle of two-way SMS can be divided into 4 main steps 1. User sends request to SMS gateway 2. SMS gateway forwards request to application server 3. Application server processes request and responds to SMS gateway 4. SMS gateway forwards request back to user mobile.

8.1 Two way communications Versus One way Communication

In contemporary, using one way communication for authentications. In one way communication is a good technique but a few drawbacks are obtained when assess than two way communications. In theft or hack in database... if the conformation codes are sent through the user mobile its saves all substantiation codes in databases. If the hijacker is easy to hack the databases and enter the code in pc so it's here security and protection altitude is low. On the other hand in two way communications it's also stored the user details in databases. But here, the hijacker will hack or theft the codes but not access because it's all access in user mobile so, it's one of the huge benefit in two way communications techniques.

9. SYSTEM DESIGN

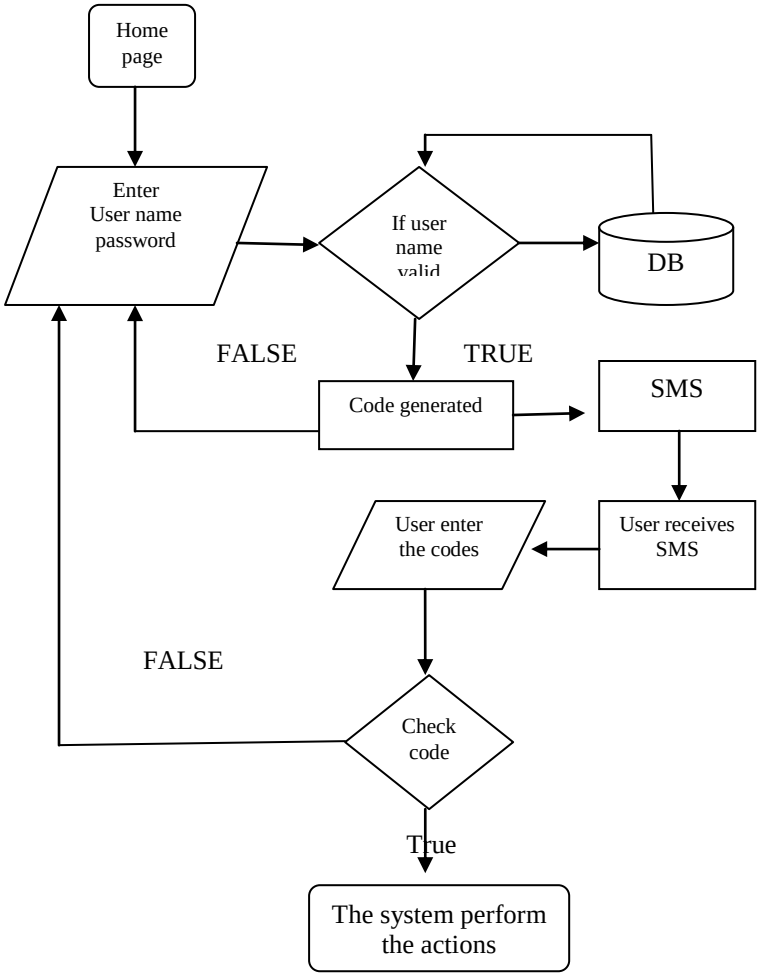

Fig 8: flow chart of PAST Progress

10. FEATURE OF 2 WAY AUTHENTICATION SYSTEMS

10.1 Double-criterion to check the identity of the User*:*

It provides a cost-effective solution to provide the web resources with a double-criterion authentication system. [1] Through a browser, a user requests permission to access a Web resource which needs an additional authentication code required for the Web Application. It then generates a [12] one-time access code and sends it to the mobile phone registered to the user by an SMS text message. The user has to enter the access code into the Web-browser to finish the authentication. After the user enters the authentication information, the system determines if the information submitted is valid or not. If valid it goes ahead with the Web Application thereby allowing the user to perform the necessary transactions, otherwise not .By separating Web Application with Authentication server, we can also divide the responsibilities to decrease the internal fraud.

10.2 Protecting the existing authentication system:

The 2WMAS 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.

10.3Protecting against internal fraud:

The system's core authentication and messaging engine is such that it provides with a good level of security to safeguard from reverse engineering and program transformation of the software. A security platform is never secured if someone has the access to the parts of the application and its security algorithm, modify the content of code to reveal security flaws or even create a backdoor entry.

11. CONCLUSION

In thesis goal was to study and implement the two way authentication method and its advantages over the one way authentication system. Our first step was analysis where we studied the traditional authentication systems and how passwords are compromised in such systems and what can be done to negate the comprising factors. This was followed with the study of the limitations of the two ways mobile authentication systems. Once the above were completed, the focus was shifted to the implementation of the two ways authentication method. High security of password, this technique will be reached in good destination and more it's really a great challenge of various hack technique as well as hijacker

12. FUTURE WORK

Probing deeper, the demo application in this thesis also provide a strong foundation for future work in Two Factor authentication for security applications. Future developments include a more user friendly GUI and extending the intense algorithm so that password can be generated based on different cryptographic functions. In addition to that we can add features such as giving as choice to the user to choose from different ways to authenticate him to the system to which he was supposed to authenticate.

13. ACKNOWLEDGEMENT

We would like to convey our thanks to our Principal Dr. **A.Syed Abu Thaheer,** for providing us with necessary facilities that enable us to successfully complete our project We are grateful to our HOD, **Prof. S. Babu Renga Rajan** for able guidance in matters and pertaining to our project. I thank him for his kindness, his interest and continued support. We would like to extend our heartfelt thanks to our project guide, **Mrs.S.Shanmuga Sundari** our project guide, for his valuable contribution, guidance and encouragement which has given us a new impetus to our work. A special note of thanks to **Mr.G. Mada Samy Raja** our project co-coordinator who rendered her support throughout the project. We owe a special gratitude to our **parents and friends** who helped us to make this project a memorable success.

14. REFRENCES

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

[2] Harris, J.A. A One Time Password Scheme .International conference on Parallel Processing Workshops, 2002 .Proceedings.

[3] Clickatell SMS Gateway developers API available at http://www.clickatell.com/developers/api_http.php

[4] FIPS 180-1 announcing standards for secured hash algorithm available from http://www.itl.nist.gov/fipspubs/fip180-1.html

[5] B. Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley, 2nd Edition, 1995.

[6] Michael Pearce, Ray Hunt, Sherali Zeadally. Assessing and Improving Authentication Confidence Management, University of Canterbury, New Zealand and University of the District of Columbia.

[7] Suzumura T, Trent S, Tatsubori M, Tozawa A, Onodera T. Performance comparison of Web Service Engines in PHP, Java and C,IEEE International Conference on Web Services 2008.

[8] George Schlossnagle, Advanced PHP programming.

[9] Naphtali Rishe, Khaled Naboulsi, Ouri Wolfson, Bryon Ehlmann. An Efficient Web-based Semantic SQL Query Generator .High Performance Database Research Center, Florida International University.

[10] Muhammad Saleem, Kyung-Goo Doh. Generic Information System Using SMS Gateway. Fourth International Conference on Computer Sciences and Convergence Information Technology 2009

[11] A.medrano,Online Banking Security-Layers of protection available at http://ezinearticles.com/?Online-Banking-Security---Layers-of-Protection&id=1353184

[12] Do van Thanh Jorstad, I.Jonvik, and T.Do Van Thuan. Strong Authentication with Mobile Phone as Security Token, Mobile Adhoc and Sensor Systems, 2009. IEEE 6th International Conference

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

[14] D. Ilett, ―US Bank Gives Two-Factor Authentication to Millions of Customers‖, 2005. Available at http://www.silicon.com/financialservices/0,3800010322,39153981,00.html

[15] Yu Tao Fan, Gui ping Su. Design of Two-Way One -Time-Password Authentication Scheme Based On True Random Numbers. Second International Workshop on Computer Science and Engineering 2009.