SLASE – A Secured Login Authentication System with Strong Encryption

Ibrahim Khalelulah M
Dept. of IT,
AdhiparasakthiEngg College,
Melmaruvathur.

Harun Kumar C
Dept. of IT,
AdhiparasakthiEngg College,
Melmaruvathur.

Shankar D
Dept. of IT,
AdhiparasakthiEngg College,
Melmaruvathur.

Sivakumar B
Assistant Prof,
Dept. of IT,
AdhiparasakthiEngg College,
Melmaruvathur.

ABSTRACT
The most common problem involves while the internet user logging into the website are phishing and key logger attacks. Most of the people even don't know about them. At present most of the websites and online banking system uses the password contains a word, alphanumeric and special characters which are unique for each and every user. It will contain fixed password characters only. So, It can be stolen by adversaries easily. To prevent this researchers proposed graphical scheme, secret question. In our scheme captcha is created from the server and user performing a simple mathematical operation on the captcha digit. It can be entered along with the fixed part of the password. Our proposed system has a simple UI. User can set the logic as much as possible. Our scheme is immune to the phishing, key logger and bot attacks. In furthermore to add security to our scheme we use the modified RSA crypto system [5] that uses n prime numbers for encryption and decryption of the users credential.

Keywords
Captcha, RSA algorithm, Security, Password, Authentication.

1. INTRODUCTION
At present most of the commercial and non-commercial websites provides services through the internet There are certain problem arises while using the passwords. One of well-known is there are static password [2] so they can be stolen by adversaries easily . Hackers perform some attacks including phishing and malware (record the keystrokes) based attacks in ordered to steal the users passwords. So, the password should be in dynamic [4] to avoid being stolen by hackers. Now a days many banking system instructed their customers to use highly strong passwords. But it impossible to change the password every time and set highly strong password for many sites. It will also waste the valuable time of end users.

Some others issues also involved in current login system. Most of the commercial websites are vulnerable to bot attacks. So, the hackers can automatically crawl the website and attempt brute force attack too. They can use all the possible ways to retrieve the password for the user. Hence, the online security has also become very essential.

2. BASIC IDEA
We create the login authentication system for users who are login into the website over the internet. we have created an environment works like a client and server architecture. Initially the user enter into our system. During the registration time, the user should have performs two tasks. The user enter the actual password. It will have the strings, numbers and special characteristics. Then they will choose the logical operation for their account. It will have the set of mathematical operation. However it is not limited. If the user has no idea about our system they can leave this and they will login our system using the fixed part password and then they will proceed the login by simply enter the numbers appeared in the captcha without any manual calculations. Once the user enters in our login page it will shows the captcha from server. User can enter the fixed part of their password along with the answers performed by using the logic with the numbers on a captcha digit. The important thing is the user password must having the numeric fields. So, that the user enter the calculated answers after the first numerical number on their password. Our scheme is immune to the bot attacks and key logger [3] attacks. In furthermore to add security to our scheme we use the modified RSA crypto system [5] that uses n prime numbers for encryption and decryption of the users credential details. So, whenever the hackers watch the traffic on network it will shows the encrypted message only. So, it's more difficult to analyze the actual password.

3. IMPLEMENTED SYSTEM
3.1 Server
In server side we have a captcha. It is being created by the server itself. It contains both words and numbers. Server will generate a five character captcha image and send to the client. Server has also a decryption system. So, that encrypted messages convert into the original messages. Here the system generates the strong private key for decryption.

3.2 Client
In client side we have a user login page contains both username, captcha and password text boxes. User should have enter the username, password to the login page. Once the user clicks the validate button. It will encrypt the all the details and send into the Server. In addition we have only uses the public key for the encryption purpose.

3.3 Verification
The user credential details are further being verified by the server side itself. We have a database for all the collected username, password and user logic for their account. Once the data is decrypted then it will check against the database. If it's true then only user can navigates to the welcome page.

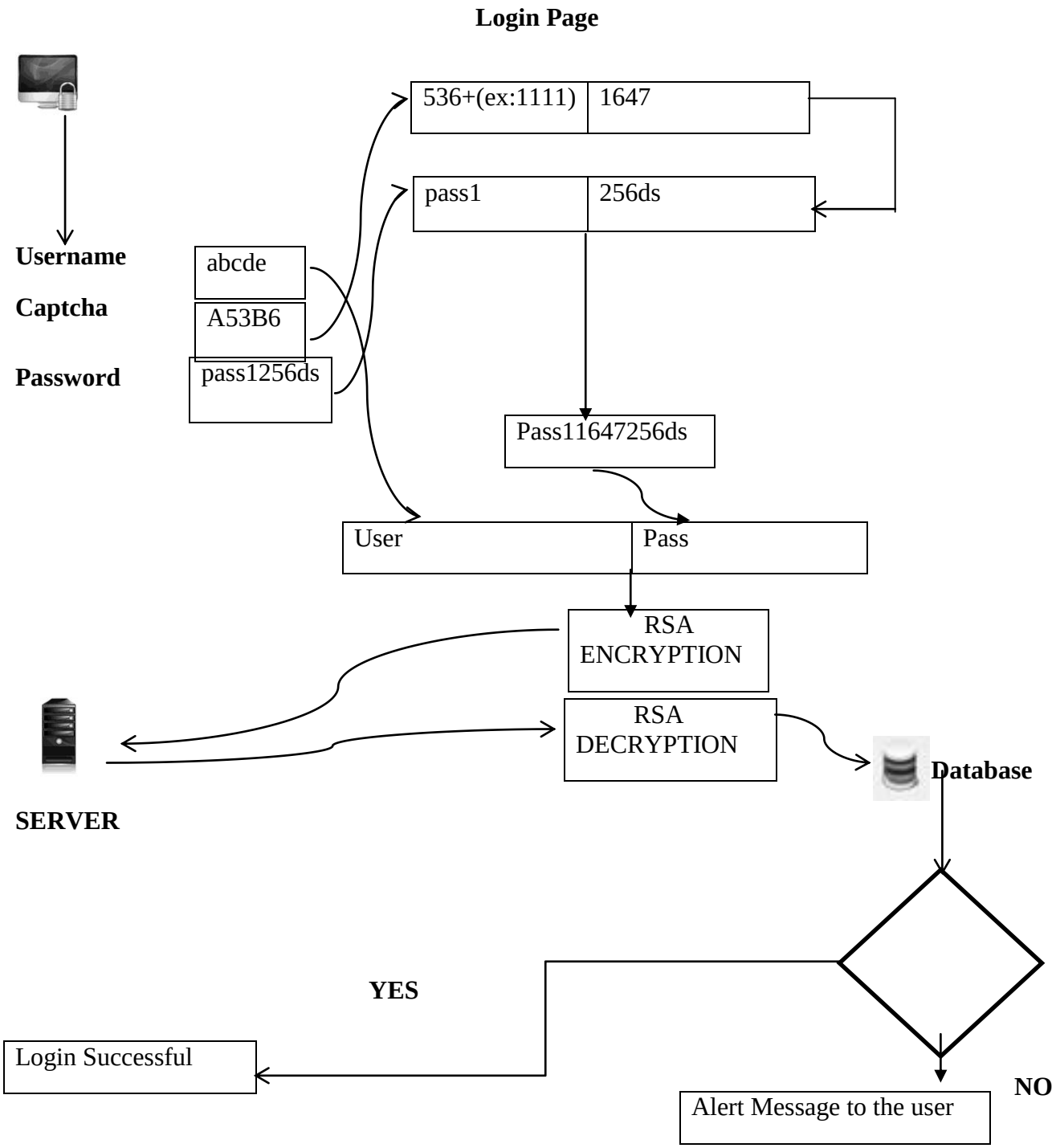

Fig 1 Architecture of the implemented system

4. COMPUTATION

Let us Consider the scenario , the user set the password logic as addition of '1111'.

- When the user login to the system , the capthca shows that '$6c7c9$'.
- Actual part of the user password is '$pas1256ds$'.
- So, the resultant password is "$pas1 + 1790 + 256ds$". (i.e.) $pas11790256ds$.
- The result will be append after the first numeric number in the fixed password field.

The password will cannot be predicted until unless if they having both captcha, user logic, and fixed part of a password.

4.1 Algorithm Used

4.1.1 Modified RSA System

We uses theRSA System based on the n prime numbers[5]. This will provides more security to the data. Here the prime numbers are not easily breakable.

Steps:

1. Select n different prime numbers p, q, r etc..

(for example here we taken the 3 prime numbers)

2.Calculate $n = p * q * r$

3.$n$used as the module for public and private key

4. Calculate $f(n) = (q-1)(p-1)(r-1)$

(where$f$ is a function of $Euler's$)

5. Select an integer e such that $1 < e < f(n)$ and

$$GCD\ (e, f(n)) = 1;$$

($e$and$f(n)$ are co-prime)

6. Determine d is multiplicative inverse of $e\ mod\ (f(n))(e * d)\ mod\ f\ (n) = 1$, d is the private key

5. SECURITY

Security is the major concern while the users login into the websites using their text password . When the user enters into our system they will login using different password each time so, the security remains high. Here the captcha is only known to the user. It can't be bypassed in case of using the bots.The advantages of using this captcha is that it can't easily hacked because it will send as the image not the actual text. In the client side we have two security method, one is mathematical operation on a captcha digit prevents the key logger attacks and the encryption of username and password. On the server side we have a strong decryption. A strong Private key is used for a decryption process. It is only known for the Server [1]. A hacker can easily read the message only if he knows the private key. So, the Algorithm we used n prime numbers RSA algorithm was more secure. The security not based on only RSA [6] algorithm it also depends upon the captcha and set of the logic.

6. SYSTEM SCREENSHOTS

Fig 2: Registration Module

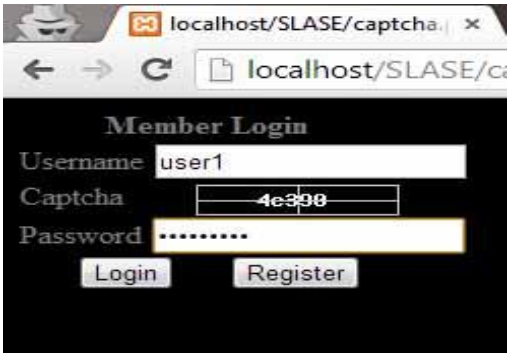

Fig 3 Login Module

7. CONCLUSION

SLASE is a secured login authentication system. It based on the captcha and user logic. So, that the user enters different password at each time. It prevents the key logger attacks and bots. It will uses the RSA [5] encryption and decryption. In such a system server plays the important role. So, the adversaries can't easily get the information from the system. Hacker can't easily hack the password. Furthermore increase system security we will use more logic for the user password.

8. REFERENCES

[1] Vivekanandan. S and John Deva Prasanna. D. S"Secured and Implicit Password Authentication toAvoid Attacks"

[2] Bhavin Tanti, NishantDoshi "A secure email login system using virtual password"

[3] Ming Lei, Yang Xiao, Susan V.Vrbsky, Chung-Chih Li, and Li Liu "A Virtual Password Scheme to Protect Passwords"

[4] DetchasitPansa, ThawatchaiChomsiri "Web Security Improving by using Dynamic Password Authentication" IPCSIT vol.11 (2011) © (2011) IACSIT Press, Singapore

[5] B.PersisUrbana Ivy, PurshotamMandiwa. Mukesh Kumar "A modified RSA cryptosystem based on 'n' prime numbers"

[6] http://en.wikipedia.org/wiki/RSA_(cryptosystem)