International Journal of Engineering Research and General Science Volume 4, Issue 2, March-April, 2016
ISSN 2091-2730

Secure Message Transmission

Babar Khalid, Shoaib Farooqui, Rajesh Nair, Priyanka Kedar

bkhalid797@gmail.com Contact no.: +919767871805
Department of computer engineering
Dhole Patil College of Engineering,
Pune Maharashtra.

Abstract: we are living on a fully digital horizon where security must be a serious threat. If you are willing to transmit confidential information over internet then you have to ensure security first. At first glans, our civilization may appear to be somewhat progressive. With the passing of everyday we are going towards the more digitized. We are enjoying fully paperless society but somewhere we are afraid of being hacked. Because it is important for person to protect owns identity from them those who are prowling in the distance. Security and privacy are the key factors if you are willing to transmitting the data over internet. we have to rethink about security of data over internet. In this paper we offered a safe zone for the customers which providing the security and privacy to the users confidential data. So, enjoy the privacy. In this paper we proposed two mechanism as 1) GRID authentication system; 2) compression and subtraction based encryption decryption mechanism.

INTRODUCTION

We are living in 21st century, a digital world. The main problem in digital world is how to protect confidential information. The first thing you want for security is authentication. So you have to protect your identity from intruders. But what if your data is stolen while data is transmitting over internet. So then you have to secure the data while data is transmitting over internet. What really occurs with data present into a computer system? However, it is also possible that something or someone within adjacent proximity to the computer read the information as well. That something or someone else might most probable be a Shoulder surfer. Dr. Fred Cohen, an esteemed frontrunner in information security and information defense organizes shoulder surfing as an occurrence that encompasses 'observing over people's shoulder as they use data or information system'.

The most mutual technique used for verification is textual password. The dimness of this technique like eves dipping, social engineering and shoulder surfing are well known. Illogical and lengthy passwords can ensure the system security. However the key challenge is it`s problematic to remember. Studies have exposed that users have an affinity to pick short passwords that are easy to recap. Inappropriately, these passwords be able to guess easily. [1] The another procedure is biometrics. But these two systems have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet broadly agreed. [2] Such configurations are expensive, and the identification procedure can be slow are two major disadvantages of these systems. There are numerous graphical password systems that are proposed in the last period. But they also suffering from shoulder surfing. [3]There are graphical password mechanisms offered which are unaffected to shoulder surfing but they have their own drawbacks like winning more period for user to login or having patience levels.

But according to our study the key problem is the attackers try to get access to the password which the user types. But what if the user does not know the password which will allow him to access? And what if user do not enter the actual password? And every time the password entered is different. Sounds a bit strange but this is what our system does. Are you afraid of being? Don't be! It's not that easy.

In this paper we proposed two techniques to protect user's confidential information. One is GRID based authentication scheme with OTP (one time password) which provide secure authentication to users.

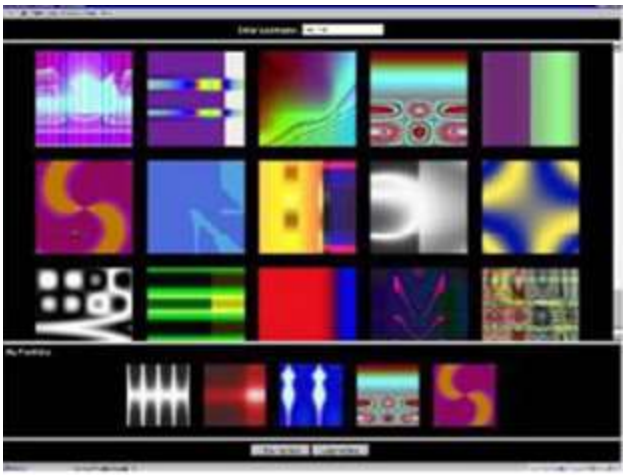
And second is for security of data over internet key exchange is the mechanism for certifying network security. For key exchange over the internet, both security and confidentiality are desired [1]. It enhances the security of the web based system and makes it difficult for the attackers to decipher the keyword of the user. This technique we can call it as cryptography. In this technique we used compression based encryption and decryption mechanism to enhance information security. And here we use DHKE as transmission security [1].

Thus, now just forget to believe that you have been lacerated and enjoy the privacy. We providing you the safe zone where your identity and confidential data are safe. So, enjoy privacy…

EXISTEING SYSTEMS

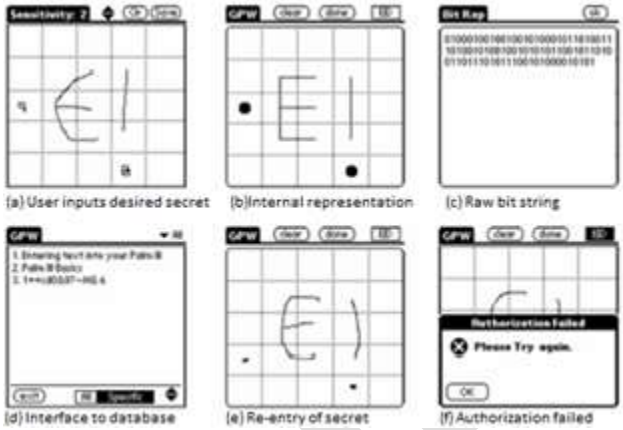
R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000[10].

Dhamija and Perrig suggested a graphical verification mechanism where user will choose images as a password to identify user's genuineness [10]. In this sytem user have to recognize the preselected images for verification at login time from a set of images as illustrated in below figure. But this mechanism has disadvantage as it is vulnerable to shoulder surfing.



Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin. "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999[12].

Jermyn Projected a new system called "Draw- a-Secret" (DAS) as described in figure where the user is necessary to draw the picture on a 2D grid. If the drawing traces the same grids in the same order as drawn during registration time, then the user is verified [12]. This system also not ensuring security from shoulder surfing.



A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441[11].

Syukri established a technique where user will draw a signature using a mouse as shown below for authorization at login time[11]. This method included two phases 1.registration and 2.verification. user draws a signature using mouse at registration time and then system extracts the signature area. at the verification time it takes the user signature as input and does the standardization and then extracts the factors of the signature. The drawback of this system is the falsification of signatures as it is not possible for users to draw a signature always as it is. It is challenging to draw the signature in the same edges at the time of registration. In this

technique the user must click on the approximate areas. So, this system is ineffective for authentication process. This system ensuring security to keystroke login but somewhere exposed by shoulder surfer.

Haich Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing[14].

Haichang offered a shoulder-surfing resilient system as shown below where the user is essential to draw a arc transverse to their password images prepared fairly than clicking on them straight. This graphical scheme chains DAS and Story arrangements to deliver genuineness to the user [14]. But this system is also vulnerable to shoulder surfing.

Suwarna jungari, Vrushali Bhujbal, Shital Sonawane, prof. Shital Salve: "authentication session password scheme using texts and colors", 2014[8].

S. Jungari offered a pair based authentication system in which User has to enter the password dependent on secret pass. The session password holds of letters and digits. Here intersection of pair is selected to submit as a password. Row of first letter and column of second letter where interacting is selected to submit the password. The intersection letter is part of the session password. This is repetitive for all pairs of secret pass [8]. This system is resistant to keystroke login but it is vulnerable to shoulder surfing.

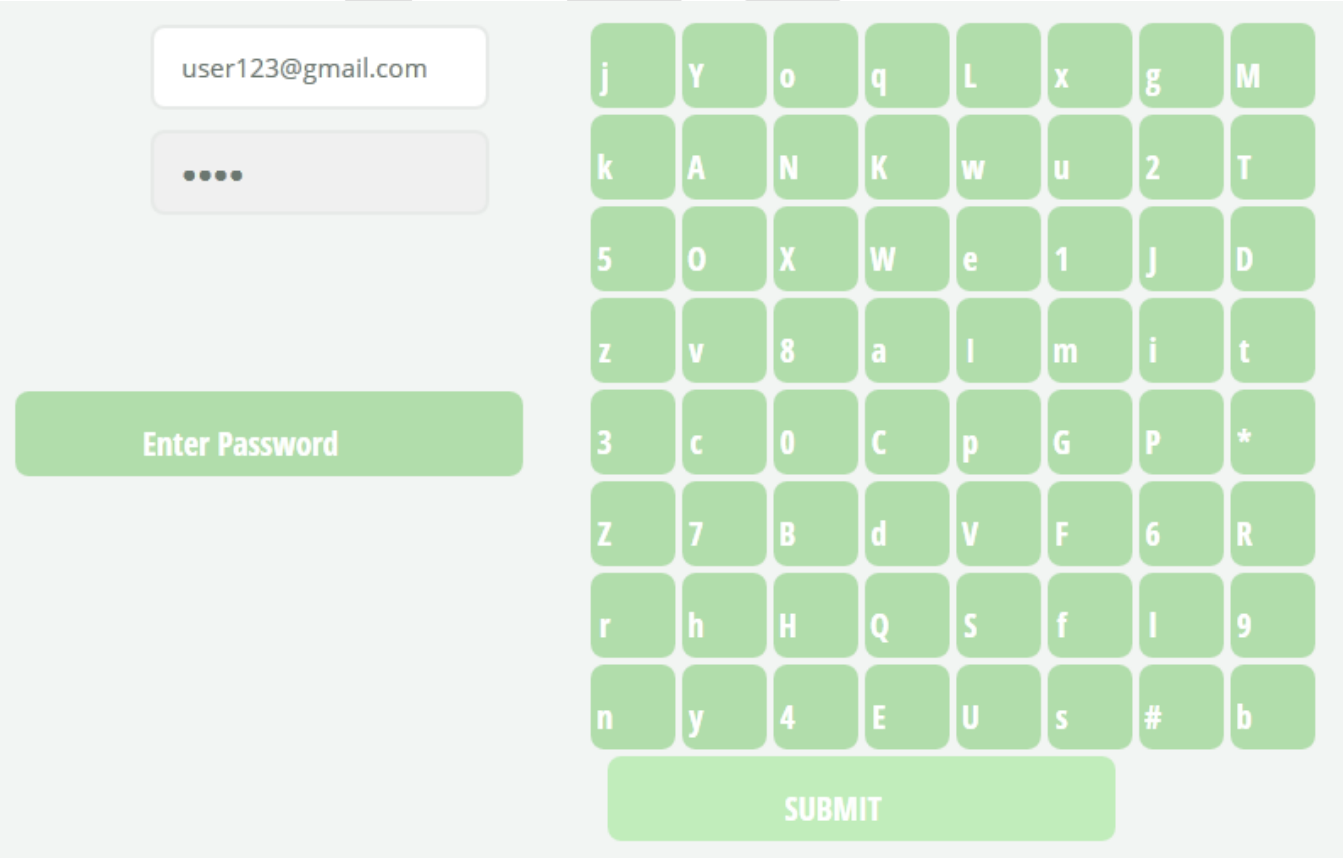
Proposed system:

Here we proposed pair based authentication system with OTP (one time password). Proposed authentication system is similar to pair based authentication system but in proposed system we eliminated disadvantages of pair based system.Pair based system has disadvantages like password must contain even number of digits while in proposed authentication system can include even as well as odd number of digits as a password. And we included OTP which is resistant to shoulder surfing and also enhance the security of the system. OTP must be included with user defined password. In proposed authentication system user have to enter predefined password as well as OTP at the time of login.

It means that for example user defined password is “asd73” and OTP received is “69” then user have to submit “asd7369” as a password in GRID. Advantage of this system is it ensures security since at every login time GRID changes.

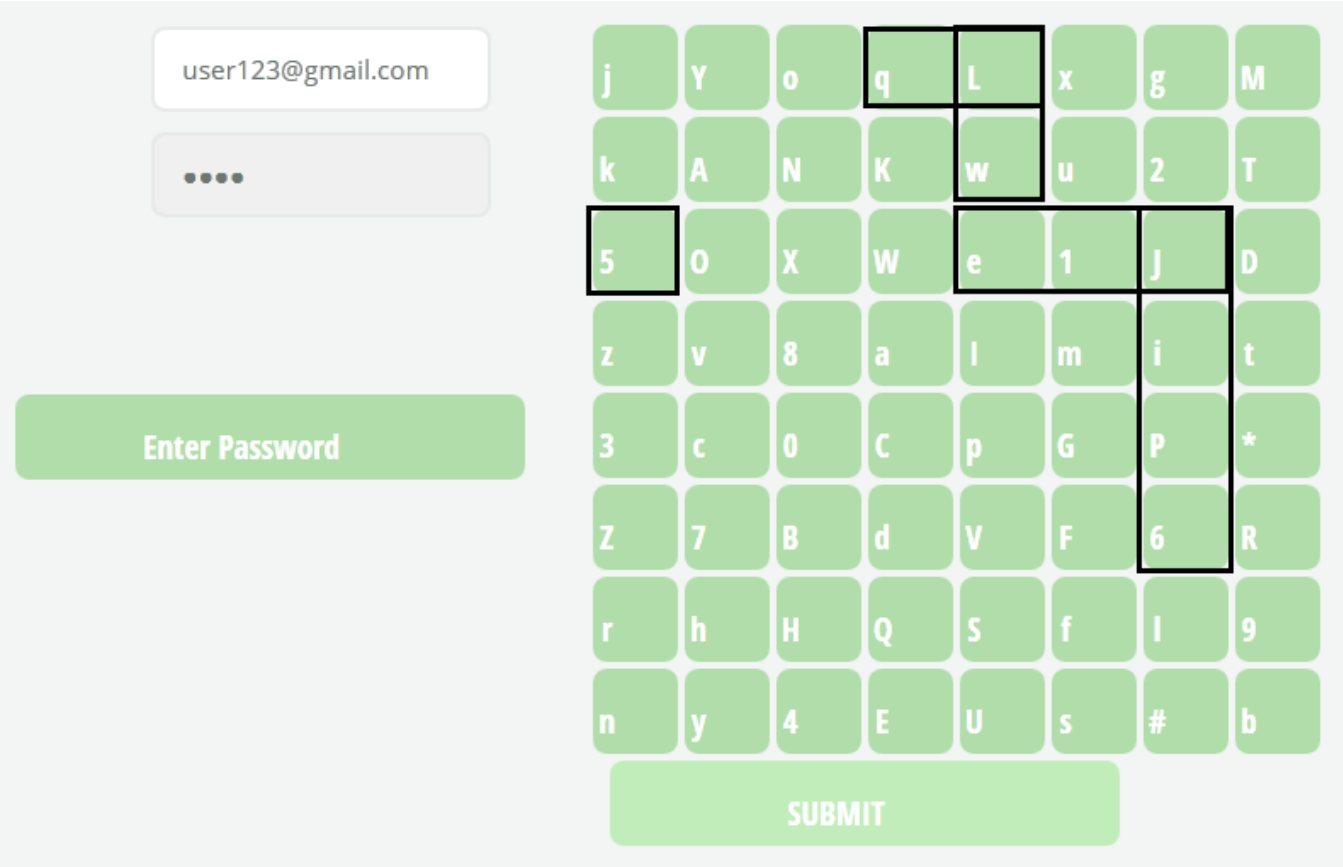
GRID contains 26 small characters, 26 capital characters and 10 digits.

26 small characters + 26 capitals + 10 digits;
26+26+10=64;
So, 64 values will be visible on GRID.



How to use

The intersection of a passwords two digits will be considered as a selection point on the GRID. It means that user have to select passwords two digits pairs intersection at login time. For example “qwe” is a user defined password and OTP received is “65” then user have to submit “LJ5” as a password as L is a intersection of row(q) and column(w) ; J is a intersection of row(e) and column(6) and 5 is selected as it is because 5 itself an intersection for 5. Which is described clearly in below figure.



Security analysis:

As discussed above GRID changes every time so that it is ensuring security. This mechanism is resistant to shoulder surfing, keystroke login and hidden camera attack due to dynamic password. Every time user get OTP and every time user submit password is always differ. So, this nature of authentication ensuring more security according to previous authentication systems.

Shoulder surfing: in proposed authentication system Grid is used where user do not submit actual password and user also enter OTP at login time. So, that system is resistant to shoulder surfing attack or hidden camera attack. Every time GRID changes and it will resistant to guessing as well.

Keystroke login: this system is resistant to keystroke login as here user submit password using GRID and keyboard interface is not needed in this authentication system.

Existing authentication system vs proposed system:

Objectives	Textual	Graphical	Biometric	Draw a secret	Proposed system
Implementation	Easy	Quit complex	Complex	Complex	complex
Accuracy	High	High	Low	Low	high
Security	Low	Low	High	Moderate	high
Hardware required	Not required	Not required	Required	Not required	Not required
Memory required	Less	Moderate	more	Less	Less
Cost	Low	Moderate	High	Low	Low
Time required to authenticate user	Less	More	less	More	less

Key exchange mechanism:

The key exchange is between the core cryptographic mechanisms for certifying network security. For key exchange over the internet we have to ensure security and privacy [1]. The internet key exchange protocol to ensure internet security, which state key exchange mechanism used to produce common keys for use in internet protocol security standard [3]. If you are willing to transmit the confidential information over internet then you have to worry about security and privacy of your information. Security is first element for information over internet. Information security over internet is serious threat now a days. Today we are living in a fully paperless world and that's why we have to rethink about security of data over internet.

Deniable internet key-exchange

[1]Andrew chi-chih Yao and Yunlei Zhao proposed family of privacy-preserving authenticated DHK[1] Protocols titled deniable Internet key-exchange (DIKE), both in the traditional PKI situation and in the identity-based setting. The newly established DIKE protocols are of intellectual simplicity and real-world adeptness. They deliver useful privacy security to both protocol applicants, and growth innovation and new assessment to the IKE conventional [3] [4] and the SIGMA protocol [5].

Internet Key-exchange (IKE)

One of the simple safe communication mechanism is key formation protocol that is known as Internet Key Exchange (IKE). It is the characteristic of Internet protocol Security (IPSec) offered by the IETF in 1998 [3, 4]. But, people have many blames for this protocol, generally for its complication [6]. The IKE and IPSec used to deliver safekeeping services and confidentiality for communication protocols. The standard of IKE has gone over two generations. 1) IKEv1 [3] uses public-key encryption as the verification mechanism. 2) IKEv2 [1] uses signatures as the authorization mechanism, with the SIGMA protocol [5] as the basis.

Internet Protocol Security (IPSec)

IPSec is the Internet Engineering Task Force (IETF) suggested standard for "layer 3 real-time Communication securities [6]." In a real-time security classification, an initiator, called Alice, establish communication session with a responder system, called Bob. They substantiate to both by verifying awareness of some secret, and then launch a secret key for the safety of the rest of the session. We use the word "real-time" to separate it from a procedure such as protected e-mail, in which Alice be able to generate an encrypted, signed message for Bob without interrelating with Bob [4].

By functioning under layer 4, IPSec preserve the problem of an active attacker critically breach at a distance a session by injecting a single volatile package. Solutions like SSL, which function above TCP, are exposed to this risk. While IPSec can be well-ordered without modifications to applications, the power of IPSec cannot be cracked till the API is altered to notify requests of the endpoint identifier, and applications are reformed to use the data in the altered API.

Proposed system

The main goal of proposed system is to enhance the security over transmission of data and authentication process in web applications. It makes difficult for the attackers to decipher the keyword and ensures the security of information navigating over internet.

Proposed system provide a safe zone to users who willing to transmit their confidential information over internet. Here we are using grid based authentication with OTP as a front end security. Here user register his/her user name and password at registration

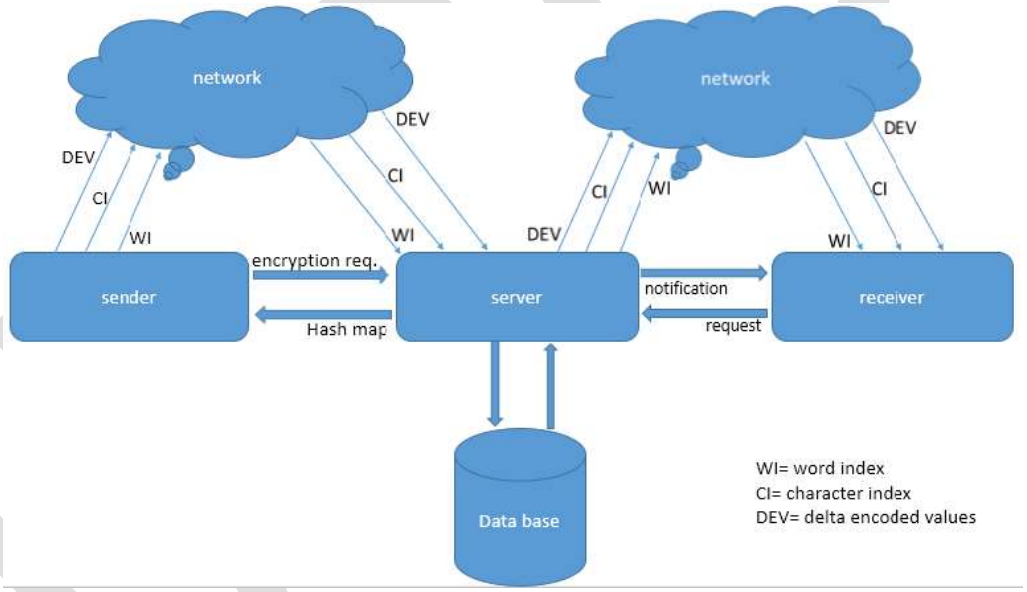
time. And at the login time user have to submit user name and password. Here user submit password using GRID. Password contains user defined password + OTP (received by message).

For example, user selected password is "qwe45" and OTP received is "65", then user have submit password "qwe4565" in GRID.

At the back-end we provide a security to user's confidential data transmitting over internet. Here we developed a new encryption and decryption technique for ensuring security to data from attacker to decipher. In this system original message is divided into three portions as word index, character index and delta encoded value as described below:

- Here we get word index as each new word typed will get assigned a word index number (wi).
- But if word types is already in the list then it will stored in to compressed list.
- If all the words got appropriate values then we proceed to character index.
- Now we assign a new character index (CI) value to each character in the word which is differ otherwise equivalent CI as assigned to same words.
- Now we will proceed to delta encoded value and fetch the hash map value (generated and received from server) of each character and then we assign first character value as same as in the hash map. And then second characters hash map value will be minimized from first character hash map value. And then this new value will be used to minimization of next characters hash map value.
- This process will be followed for all the characters in the message and then what we will get is the delta encoded value.
- Now all values (word index, character index, and delta encoded value) are to be append one value to a one individual message. At the last all the values are to be sent as an individual message for security enhancement.
- Now whenever server get message from the sender it will notify the appropriate receiver about message.
- Now whenever receiver login to the system and request for the message, server will send ciphered text (WI, CI, and delta encoded value) to the receiver system And delete that message from the server to enhance the information security.
- Then decryption takes place at the receiver system and original message will be sent to the receiver by e-mail.

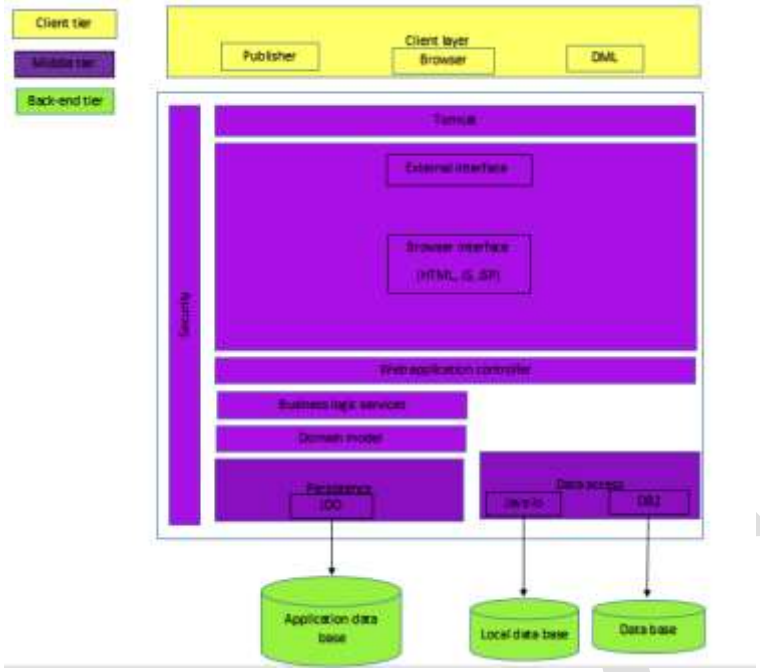
This process is clearly described in below figure.



Message entered by user is encrypted at client side and then ciphered text is sent to server and stored on to the server. Server store encrypted message in message data base and then notify appropriate receiver about message. Whenever receiver login into the system and request for the message, server sent ciphered values to the receiver and decryption take place at the receiver end. Then original message will be sent to receivers email address.

System architecture:

A system architecture is the theoretical model that explains the structure, activities, and more understandings of a system. Architecture view is describe all technologies and interfaces used for implementation of this system. The fundamental body of a structure, their associations with each other and to the atmosphere, and the ethics leading its intention and evolution. A detailed system architecture is illustrated in below figure.



MATHEMATICAL MODEL

U= {U1, U2, U3 ...Un} (User)
S= {Server} (Server)
M= {M1, M2, M3 …Mn} (Message)
K= {K1, K2, K3 ...Kn} (Key)
HT= {HT1, HT2, HT3 ...HTn} (Hash Table)
RN= {RN1, RN2, RN3...RNn} (Random no.)
DEV= {DE1, DE2, DE3...DEn} (Delta encoded values)
WI= {WI1, WI2, WI3 ....Win} (word index)
CI= {CH1, CH2, CH3 ...CHn} (character index)
DB = {Udb, Mdb} (data base, user data base, message data base)
L= {success, failure}
MTG= {U, S, M, K, HT, RN, DEV, WI, CI, DB, L}

Compression based message encryption

Here we will see how message encryption mechanism work when user enter original text message.

Whenever user select to send the message at the same time server generate grid and send GRID value to the client machine. Now as user submit their original text message client machine start encryption process. How mechanism work is as follows:

Let word token WT=n; current character k=0; stored array j=0; word index WI= i; character index CI= empty; and then three events will be followed by mechanism to encrypt the message.

Event 1:

Now read the text message and if space arrived in the text we will consider it as a word-end. So, word token is increased by 1. So, now $WT_n=WT_{n+1}$.

And then if word previously read is in not registered in the list then WI=i+1; otherwise store word into compressed list and increase token WT_{n+1}.

This process is followed by all the words in the text message and what will produced is word index of all words from the text message.

Event 2:

Now here access the word array created in event 1. And split words into characters and let current character as k; current character index CI=y; CI (k) =x;

Now read characters one by one and increase CI (k) =y+1 if k is not there in the CI array. Else CI (k) = CI(x). Follow this steps for all characters present in the text and we will get character index of all characters.

Event 3:

Now assume q= current character; hash-map value=HM (q) =q_{ij} (i^{th} and j^{th} location of q in the hash-map); delta encoded value (q) =DEV (q) =empty; and p=previous characters DEV;

Now DEV (q) =HM (q) if and only if DEV (q) =empty;

Otherwise DEV (q) = (DEV (p) - HM (q)).

This step is followed by all the characters in the text and we will get delta encoded value.

Hence, at the end of the three events we got WI, CI, and DEV. And message is encrypted successfully.

Results

Authentication:
Below chart illustrate the result of user login time as how much time system takes to authenticate the user at login time. It describe the time taken by system to authenticate the different users. This time also depend on network speed.

users	Time(ms)
1	10
2	9
3	10
4	11
5	9
6	10
7	9

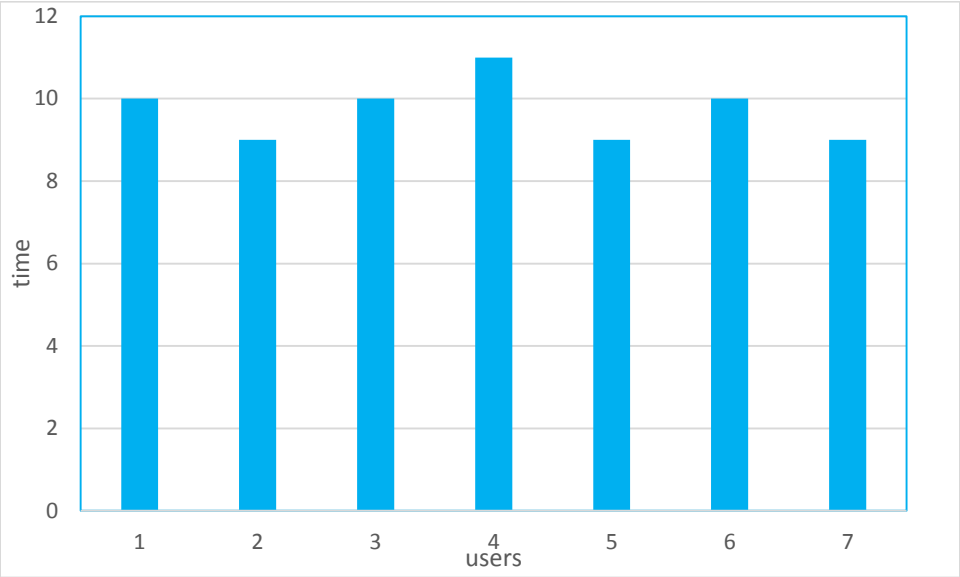


Chart shown above is describing the result in terms of login time. it shows how much time taken by system to authenticate which user. It shows time taken by system to authenticate 7 users.

ACKNOWLEDGMENT

We are grateful to prof. Priyanka Kedar for very supportive clarification and suggestions, as well as very helpful suggestions about this project.

Conclusion

In this paper, we proposed a safe zone for the user willing to transmit confidential information over internet. Here we proposed message encryption technique for ensuring data security over internet which is followed by GRID based authentication system using OTP which is resistant to shoulder surfing as well as keystroke login.

REFERENCES:

[1] A. C. Yao and Y. Zhao, "privacy-preserving Authenticated Key-Exchange over Internet" January 2014.

2] S. Al-Riyami and K. Paterson, "Certificate less public-key cryptography," in *Proc. Asiacrypt 2003, pp. 452–473.*

[3] D. Harkins and D. Carreal, "The Internet key-exchange (IKE)," IETF (The Internet Engineering Task Force), New York, NY, USA, Tech. Rep. 2409, Nov. 1998.

[4] C. Kaufman, "Internet key exchange (IKEv2) protocol," The Internet Engineering Task Force, London, U.K., Tech. Rep. 4306, Dec. 2005.

[5] H. Krawczyk, "SIGMA: The 'SIGn-and-MAc' approach to authenticated Diffie-Hellman and its use in the IKE-protocols," in Proc. CRYPTO 2003, pp. 400–425.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Proc. CRYPTO 2001, pp. 213–229.

[7] A. C. Yao and Y. Zhao, "Deniable Internet key-exchange," IACR (The International Association for Cryptologic Research), San Diego, CA,USA, Tech. Rep. 2011/035, Jan. 2011.

[8] Suwarna jungari, Vrushali Bhujbal, Shital Sonawane, prof. Shital Salve: "authentication session password scheme using texts and colors", 2014.

[9] VAISHNAVI PANCHAL, CHANDAN P. PATIL a user study using "Authentication schemes for session password" March 2013.

[10] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

11]A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[12]Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin. "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.
[13] Real User Corporation: Pass faces, www.passfaces.com.

[14]Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing

[15] M SREELATHA , M SHASHI , M ANIRUDH "Authentication Schemes for Session Passwords using Colour and Images" May 2011.

[16] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in Proc. CRYPTO 1993, pp. 273–289.

[17] Babar Khalid, shoaib Farooqui, Rajesh nair, Priyanka Kedar, "privacy for key exchange and authentication process using grid", IJSRD/vol. 3,issue 09,2015/ISSN:2321-0613