Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 11, Number 6 (2015), pp. 4375-4384

http://www.ripublication.com

An Effective Method for Preventing Hackers using Biometric Techniques

S Igni Sabasti Prabu

Asst. Prof, Faculty of Computing Sathyabama University, Chennai, India.

Abstract

Security is the major concern in today s world. Web services are large in number and the security system to prevent intrusion in the system is also growing. The intruders find loopholes to break the system. So it is better to strengthen the system security by not only using some software systems but also to bio metric dynamics to stop the intruders. The proposed system provides a way to protect the system from intrusion using key stroke biometrics and thereby detect the anomalies inside the system and also to detect the attackers outside the system.

Keywords: Anamolies, Biometric, Intruder, Security, Web services

I. Introduction

With the growth of the internet as a premier means of communication, a new paradigm called web services has emerged. Web service offers various functionalities in the area of communication, e-commerce, banking, insurance, marketing, health and social networking among others. Due to the proliferation of web services, obviously, many service providers volunteer themselves to create and publish business processes as services. Internet is a huge resource library for clients and service providers to locate and access the business services. Furthermore, enterprises outsource their internal business processes into web services and make it available to web. Therefore, many services are available for similar functionality to satisfy a request. Any service is liable to attacks. Securing a web service is a major task. As Green IT has been issued, many companies have started to find ways to decrease IT Cost and overcome economic recession. It is efficient and cost economical for consumers to use computing resources as much as they need or use services. Especially, web services have been recently more spotlighted than other computing services because of its capacity of providing unlimited amount of resources. Moreover, consumers can use the services wherever

internet access is possible, so web services have lot of resources and private information; therefore they are easily threatened by attackers. Especially, system administrators potentially can become attackers. Therefore, providers must protect the systems safely against both insiders and outsiders. Next we discuss about Keystroke biometric analysis:

- Keystroke dynamics is the process of analyzing the way a user types on a keyboard and identify him based on his habitual typing rhythm
- A user's typing pattern may be unique because similar neuro-physiological factors that make written signatures unique are also exhibited here
- Keystroke dynamics is a behavioral biometric
- Natural choice for computer login and network security Keystroke DynamicsKeystroke Dynamics

Keystroke dynamics is not what you type, but how you type Features commonly used to describe a user's typing pattern are. Latencies between successive keystrokes (the elapsed time between the release of the first key and the depression of the second)Duration of each keystroke (How long is the key held down). Pressure applied on the keys. Overall typing speed. For known regularly-typed strings (e. g., username and password), such features are quite consistent. However, features are a function of the user and the environment

Advantage:

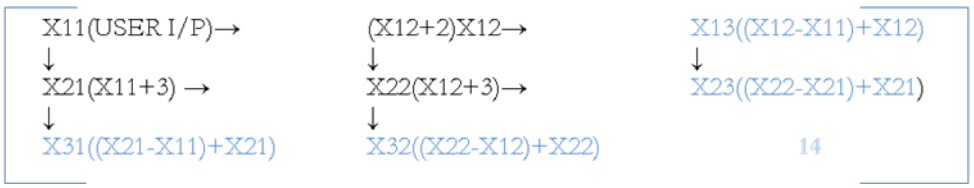
1. Cost efficient no additional hardware
2. Non intrusive and wide user acceptance
3. Natural authentication mechanism for computer and network security continuous verification (monitoring) is possible.

This paper is organized as follows: section 2 describes Proposed System, section 3 presents the Implementation and Results. Finally in section 4 the paper presents some conclusion.

II. Proposed System

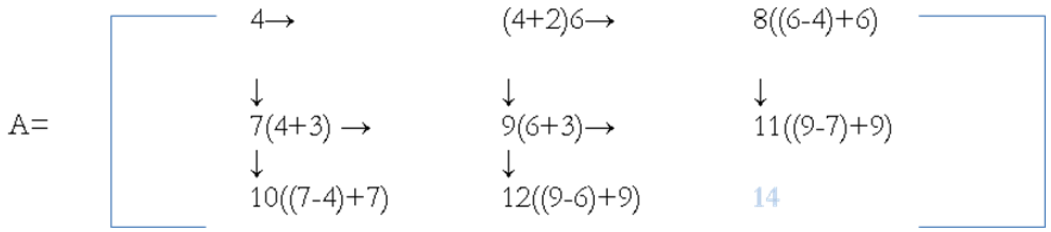
The system architecture of the proposed system is shown below. The user is authenticated by the admin before he enters the system. The admin then checks the IP address. The maximum connection attempt of a user is limited to five attempts. The user during his registration has to calculate typing speed. Each time the user logs in with the username and password, a session key is generated and sent to the user through SMS. The admin maintains a log of the user. The log details are Username, password, IP address, MAC address, session key, the login time, the no: of connection attempts and also the typing speed. The time in which the user logs in is also maintained so as to know if the user accesses the web service in the working time or later. The validation of the client is done with the help of matrix encryption. The matrix encryption algorithm is as follows

Principle:
To form a (3*3) matrix from a user input in such a way that all the elements of matrix are related so that its determinant value becomes zero



The blue colored elements on the above matrix are multiplexed using or gate and Stored in the database for the corresponding user during registeration. for each and every Login user makes the correspondin value for user i/p is calculated and verified with the stored one.
X11(X)+x12(Y)=x13->1
X21(X)+x22(Y)=x23->2
X31(X)+X32(Y)=X33->3
SOLVING 1 AND 2 :
WE X AND Y
SUBSTITUE X AND Y IN 3 WE GET X33 VALUE
x33 value is the one which makes the det of matrix=0

EXAMPLE:



Steps :
1. Admin has to allow the User to access the Cloud after its Authentication
2. It will check the Host / Guest IP Address.
3. If a user takes more than 5 attempts for Authentication, then a alert is registered in his account.
4. If a user sends some Malicious Code to the cloud server.
5. User has to give proper Session Key which is generated via SMS to the User's Mobile number.
6. Attempt of the user after working hours.
7. User machine's port number is also verified.

The attackers are easily identified with the help of keystroke dynamics and the validation of the user is strengthened with the help of the matrix algorithm.

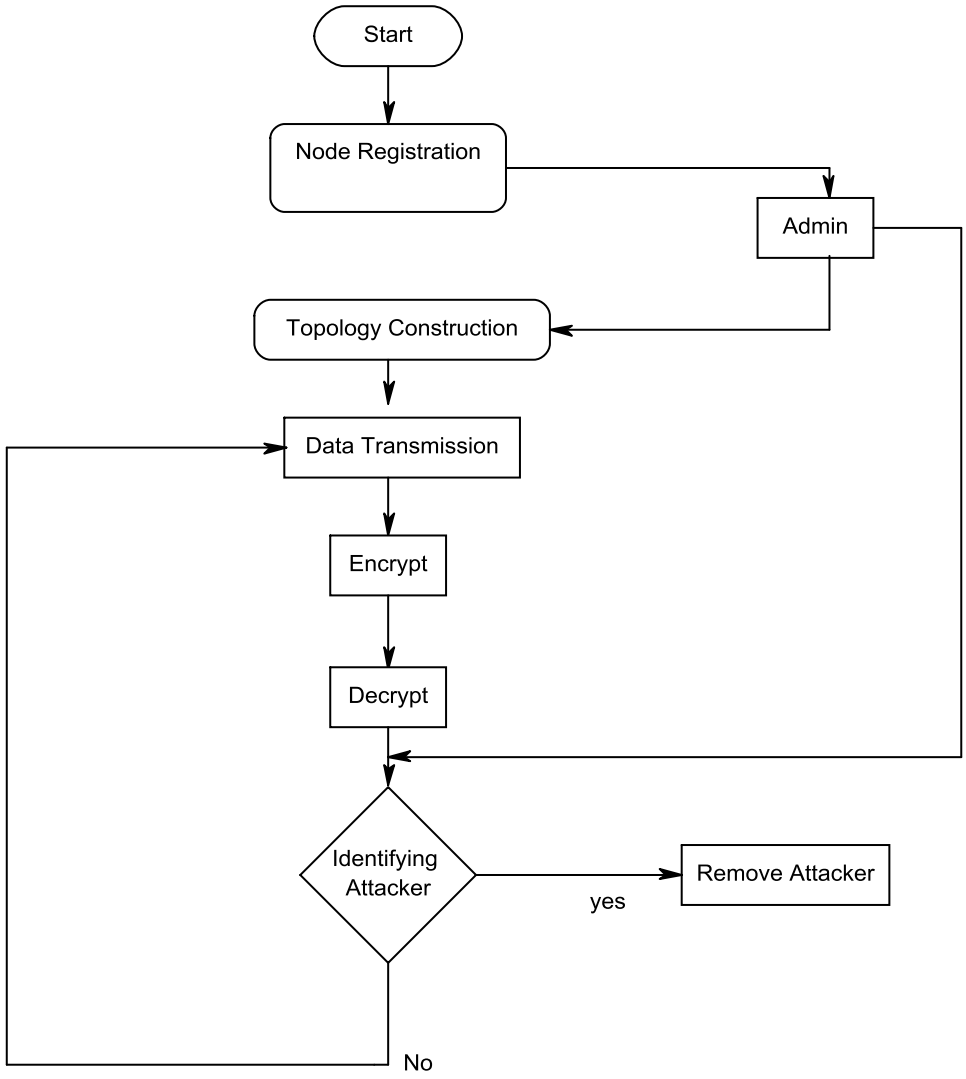


Fig. 1. System Architecture

III. Implementation and Results

The experiment was implemented in a bank database. The client logs in and with the inputs the mat value is calculated and the client is authenticated and he can start his transaction. The user registers first and each time he wants to sent a query the user has to login and he is validated and the typing speed is calculated. The attackers are identified in the level of authentication itself.

Algorithm for Validation

VALIDATE(USERNAME1, PASSWORD1, IP1, MAC1, SESSIONKEY1, TYPINGSPEED1, SESSIONTIME)

Begin

RETRIEVE(USERNAME, PASSWORD, IP, MAC, SESSIONKEY, TYPINGSPEEDSESSIONTIME)
USERNAME=A
PASSWORD=P
IP=I
MAC=M
SESSIONKEY=S
TYPINGSPEED=T
SESSIONTIME=ST
If(USERNAME1=A, PASSWORD1=P, IP1=I, MAC1=M, SESSIONKEY1=S, TYPINGSPEED1=T, SESSIONTIME=ST1)
SEND(SUCCESS)
Else
SEND(FAILURE)
ALERT(MSG)
EndIf
End

RETRIEVE(USERNAME, PASSWORD, IP, MAC, SESSIONKEY, TYPINGSPEEDSESSIONTIME)
1. CONNECT TO DATABASE USING TYPE1 JDBC CONNECTOR
2. IF THE PARAMETER RECEIVED MATCHES THE RETRIEVE THE VALUES FROM DATA BASE USING STATEMENT AND STORE TEMPORARILY IN RESULTSET
End

VALIDATEUSER(USERNAME, PASSWORD, MATVALUE)
Begin
USERNAME=U
PASSWORD=P
MATVALUE=M
RETRIEVE(USERNAME, PASSWORD, MATVALUE)
If(USERNAME=U, PASSWORD=P, MATVALUE=M)
SEND(SUCCESS)
Else
SEND(FAILURE)
EndIf

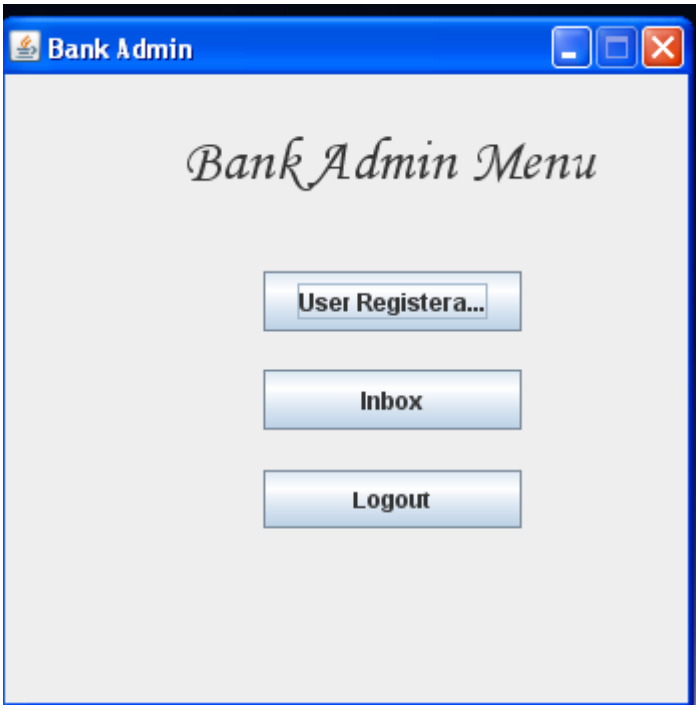


Fig. 2. Bank Menu

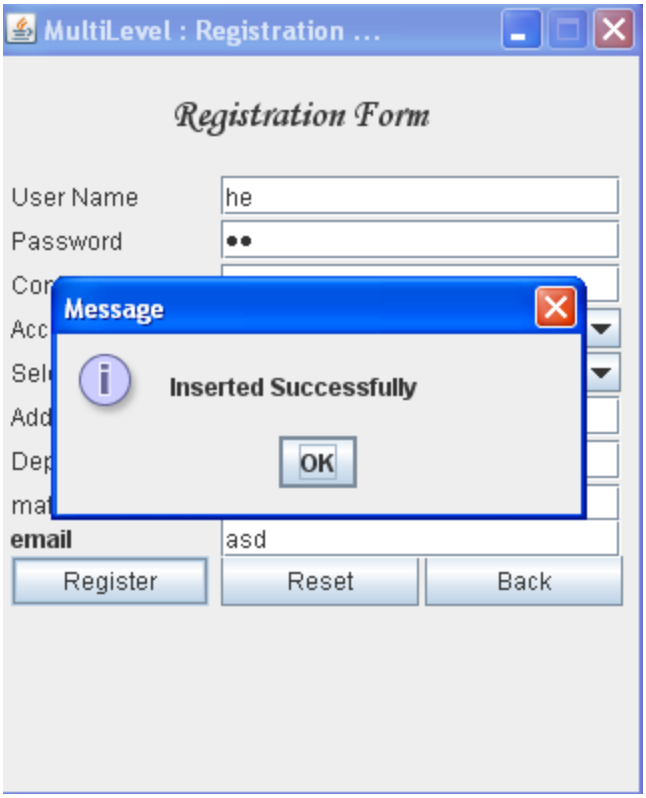
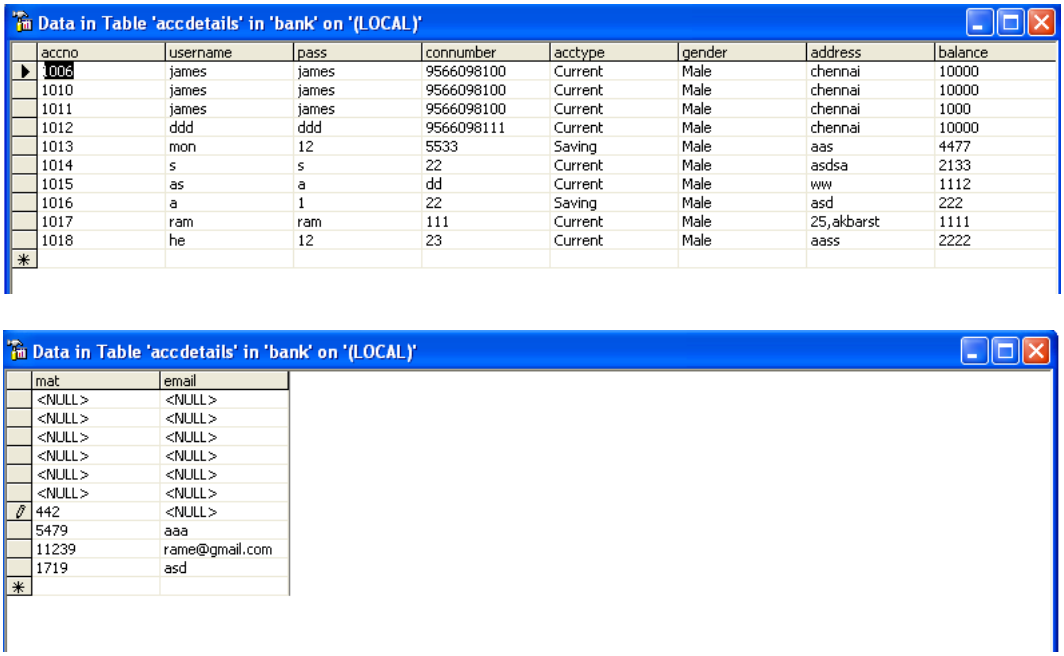


Fig. 3. Registration Form



Data in Table 'accdetails' in 'bank' on '(LOCAL)'

accno	username	pass	connumber	acctype	gender	address	balance
1006	james	james	9566098100	Current	Male	chennai	10000
1010	james	james	9566098100	Current	Male	chennai	10000
1011	james	james	9566098100	Current	Male	chennai	1000
1012	ddd	ddd	9566098111	Current	Male	chennai	10000
1013	mon	12	5533	Saving	Male	aas	4477
1014	s	s	22	Current	Male	asdsa	2133
1015	as	a	dd	Current	Male	ww	1112
1016	a	1	22	Saving	Male	asd	222
1017	ram	ram	111	Current	Male	25,akbarst	1111
1018	he	12	23	Current	Male	aass	2222

Data in Table 'accdetails' in 'bank' on '(LOCAL)'

mat	email
<NULL>	<NULL>
<NULL>	<NULL>
<NULL>	<NULL>
<NULL>	<NULL>
<NULL>	<NULL>
<NULL>	<NULL>
442	<NULL>
5479	aaa
11239	rame@gmail.com
1719	asd

Fig. 4. Database of users with encrypted mat value

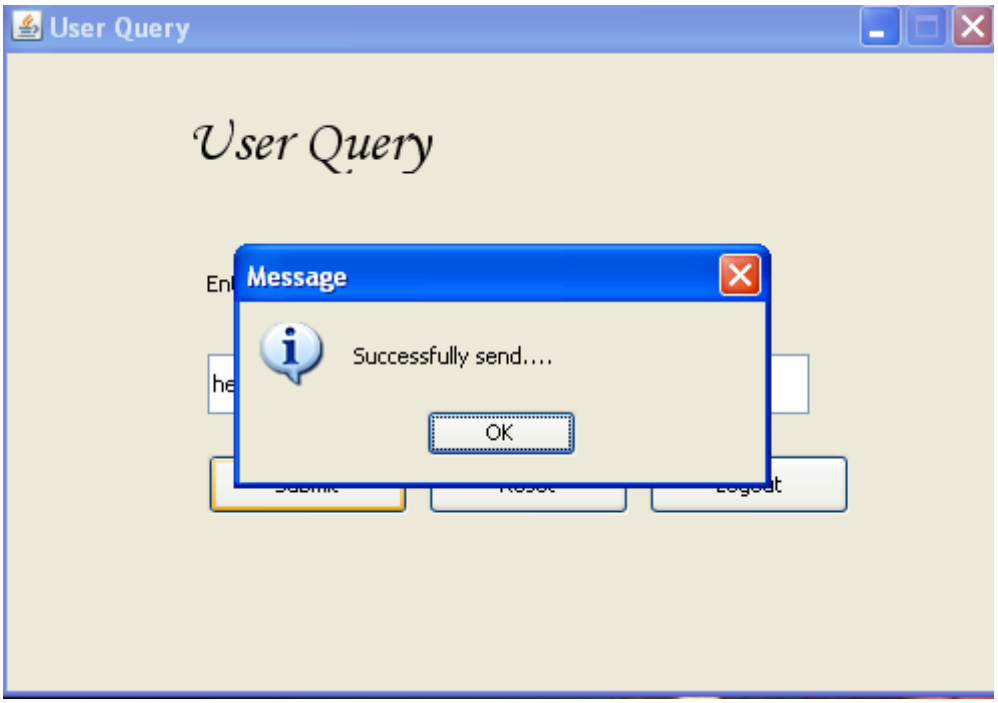


Fig. 4. user query

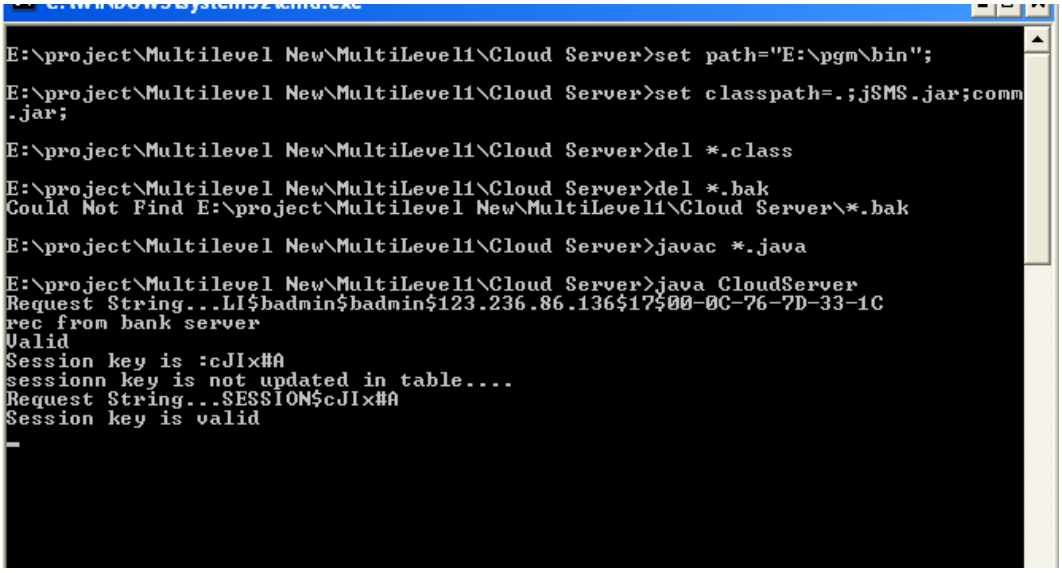


Fig. 5. Session Key

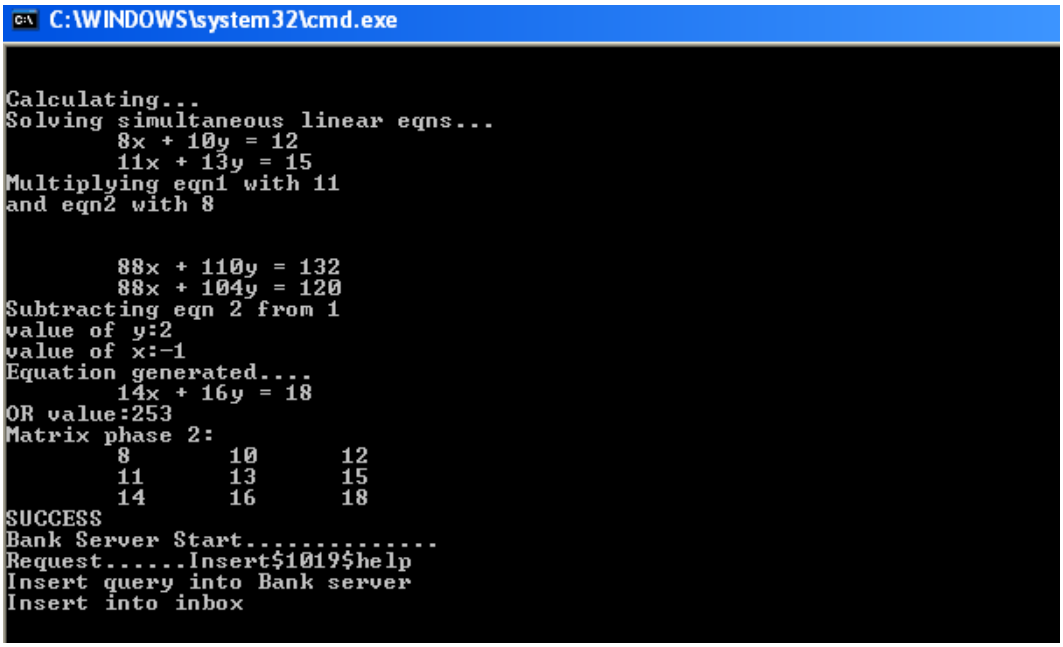


Fig. 6. Mat value calculation

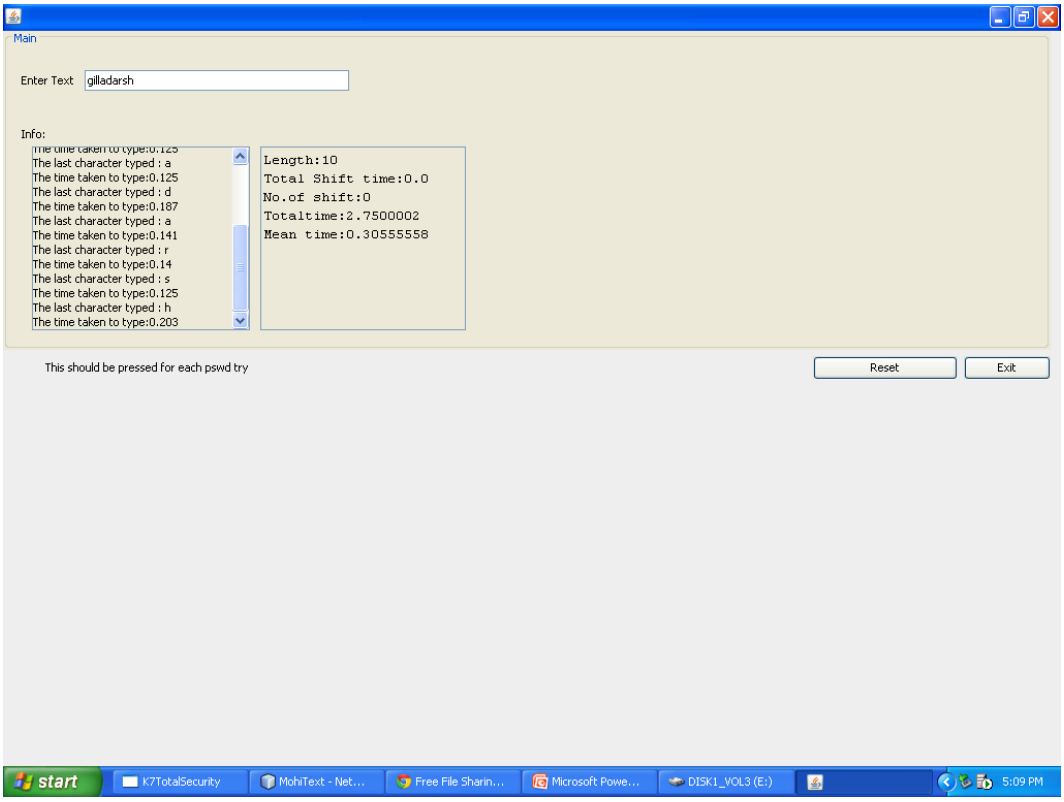


Fig. 7. Typing speed calculation

IV. Conclusion

Web services security must be a continually evolving process. If there is a security accident the economic damages are inevitable. There is not only loss of data but also loss of confidentiality and thereby we lose valuable customers. In the paper we have combined the matrix encryption algorithm and the key stroke dynamics to identify the attackers. And hence secure the web services.

References

[1] *Edmond Lau, Xia Liu, Chen Xiao, and Xiao Yu Enhanced User Authentication Through Keystroke Biometrics, Computer and* Network Security, Massachusetts Institute of Technology, December 2004.

[2] Jun-Ho Lee, Min-Woo Park *Multi level Intrusion Detection System and Log Management in Cloud Computing,* ICACT2011

[3] M. Hamdi and N. Boudriga, "*Detecting Denial-of-Service attacks using the wavelet transform,* " Computer Communications vol. 30, p. 10, 2007.

[4] *C. Callegari, S. Giordano, and M. Pagano,* "Application of Wavelet Packet Transform to Network Anomaly Detection, " in Next Generation Teletraffic

and Wired/Wireless Advanced Networking: 8th International Conference, NEW2AN 2008and RuSMART, St. Petersburg, Russia, 2008, p. 246

[5] G. Liu, Z. Yi, and S. Yang, "A hierarchical intrusion detection model based on the PCA neural networks, " Neuro computing, vol. 70, pp. 1561-1568, 2007.

[6] S. Panjwani, S. Tan, K. M. Jarrin, and M. Cukier, "An Experimental Evaluation to Determine if Port Scans are Precursors to an Attack, " in International Conference on Dependable Systems and Networks (DSN-2005), Yokohama, Japan, June, 2005, pp. 602-611.

[7] D. Bolzoni, E. Zambon, S. Etalle, and P. Hartel, "POSEIDON: a 2-tier Anomaly-based Network Intrusion Detection System, " in *Proceedings of the 4th IEEE International Workshop on Information Assurance (IWIA)*, 2006, pp. 144-156.

[8] C. Xiang and S. M. Lim, "Design of Multiple-level Hybrid Classifier for Intrusion Detection System, " in *2005 IEEE Workshop on Machine Learning for Signal Processing*, 2005.

[9] *G. Song, J. Zhang, and Z. Sun,* "The Research of Dynamic Change Learning Rate Strategy in BP Neural Network and Application in Network Intrusion Detection, " 2008, pp. 513-513.

[10] *X. Ke, R. Manuel, M. Wilkerson, and L. Jin*. "Keystroke Dyamics: A Web-based Biometric Solution. " 13th USENIX Security Symposium.

[11] M. Brown and S. J. Rogers. User identification via keystroke characteristics of typed names using neural networks International Journal of Man-Machine Studies, 1993.

[12] G. Leggett and J. Williams, M. Usnick. "Dynamic Identity Verification via Keystroke Characteristics. " International Journal of Man-Machine Studies, p. 859-870, 1991.

[13] R. Gaines, W. Lisowski, S. Press, and N. Shapiro. "Authentication by Keystroke Timing: some preliminary results. " Rand Report, 1980.