Proposing 3SEMCS- Three Step Encryption Method for Cyber Security in Modern Cryptography

Manraj Singh
Department of Computer Science & Engg·
Sri Sai Institutes of Engg and Technology, Manawala (Amritsar)
Punjab-India

Amit Kumar
Department of Computer Science & Engg
Sri Sai Institutes of Engg and Technology, Badhani (Pathankot)
Punjab-India

Shubham Chuchra
Master of Computer Applications
Chandigarh Group of Colleges, Landran
Punjab-India

Navreet Kaur
Department of Computer Science & Engg·
Sai Institutes of Engg and Technology, Manawala (Amritsar)
Punjab-India

Sajan Dhawan
Department of Computer Science & Engg·
Sai Institutes of Engg and Technology, Manawala (Amritsar)
Punjab-India

ABSTRACT

Cyber security is a critical issue now a days in various different domains in different disciplines. This paper presents a review analysis of cyber hacking attacks along with its experimental results and proposes a new methodology 3SEMCS named as three step encryption method for cyber security. By utilizing this new designed methodology, security at highest level will be easily provided especially on the time of request submission in the search engine as like google during client server communication. During its working a group of separate encryption algorithms are used. The benefit to utilize this three step encryption is to provide more tighten security by applying three separate encryption algorithms in each phase having different operations. And the additional benefit to utilize this methodology is to run over new designed private browser named as "RR" that is termed as Rim Rocks correspondingly this also help to check the authenticated sites or phishing sites by utilizing the strategy of passing URL address from phishing tank. This may help to block the phisher sites and user will relocate on previous page. The purpose to design this personnel browser is to enhance the level of security by sign_in on the time of client server communication that correspondingly reduce the normal attacks on browser based attacks as like Man-

In-The-Middle-Attack (MITMA). This new designed private browser may help to provide online security by applying 3-step automatic encryption on path during request movement of google page from the one to the next or ultimately/towards web server by following auto-generated encrypted hash address approach. At end, this rim rocks browser provides tighten security with anti-phishing facility during client server communication.

Keywords

hash address, encryption algorithm, Private browser, Search Engine, Index Pointer, Uniform Resource Locator Address, and Internet, cyber-security, law Ethics.

1. INTRODUCTION

Cyber security is an interdisplinary field and act as a global problem in cyber world [11] because of internet users becomes increases day by day [42]. The area of Cyberspace [7] is treated as in the shape of hub [2] that tells the ratio of attacks performed by different categories of attackers with incents in different industries that can be shown in fig.1, 2, 3 & 4.

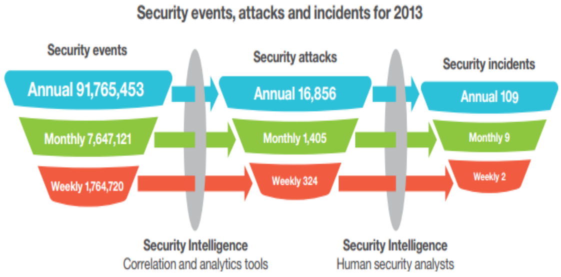


Fig.1: Effects of Security Intelligence in 2013. [38].

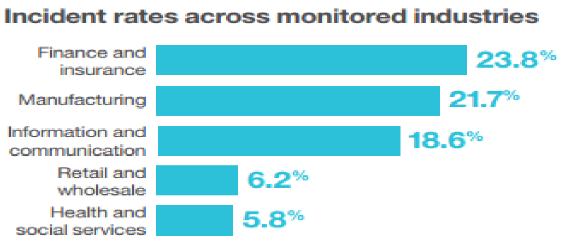


Fig.2:Potential Payoff for maufacturing and financing Industries[38].

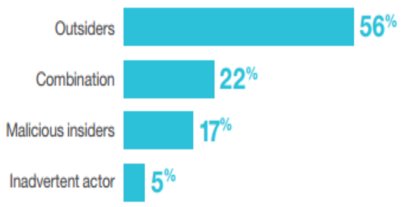


Fig.3:Categories for Attackers[38].

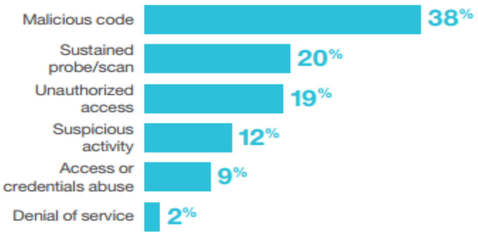


Fig.4:Categories for Incident[38].

As per changing time, trends and technologies may change correspondingly effect on the way of communication through cyber world[8] in different field's viz. knowledge, health, and commerce [29], [6], [10] during information exchange. The scope of cyber security is not just limited to securing the information in IT industry but in various other fields which are existing in cyber space [22]. The three main building blocks of cyber security is viz. confidentiality, integrity and availability [19] and the dependency of its core-pillars is based only on trust level [16] .The importance of the cyber security is to study various cyber laws[5] so that professionals will easily detect the nature of cyber-attack where cyber-attack may harm our nation's security and defend itself as well as people that may be a type of life loss in the form of theft at the levels of tens and billions[15] in the form of phishing attacks[33].Different types of phishing attacks viz. black listing, symptom based protection, content filtering[52] and domain binding[51],[57],[64],[65] are performed by the phishers for spoofed websites[47],[67]. Most commonly phishers uses link guard algorithm [48] for performing phishing. As data collected by the authors, they studied presently 7690 sites are legitimate sites and approximately 2280 sites are phishing sites [58]. Security professionals mostly uses Phish tank[58] site for detecting the phishing attacks [51],[57],[64],[65] that gives the complete information of the URL'S(Uniform Resource Locator) addresses in detail as an example this website is blocked and this is phished site- Do you want to proceed next?. In addition, phishing attacks may detected by utilizing several anti-phishing framework [56],[60],[61] or anti-phishing tools [49],[50],[53],[55] that uses CAPTCHA Image Validation check , different mobile mechanisms for anti-phishing[[54],[62] may easily detect phishing and send vibrations as well as message alerts to users. The most common method used by the security professionals for detecting phishing is honeypot method [66]. While utilizing these different methods Phished websites regular reports [68] may be generated by the security professionals. So they utilizes several methods for applying high level of security at separate levels as like on data or information [24], [25], [39], security on browser [17], security on services [18], can be most commonly implemented on different types of security controls[41],security polices [2],[9],[14],operations[32] ,ethical frameworks[4],national governmental approaches[3] etc. As with the changing trends and technologies towards digital world mostly tasks are handled by cyber world that correspondingly increase the level of risk during confidential information transfer from one end to another end. For improving the level of cyber security professionals have more need to focus on the incorporating new technological approaches in products and processes [23] as an example previously they designed a new cyber security monitoring system whose function is to integrate the number of component techniques to collect time series situation information for intrusion detection[26]. For reducing the intrusion attacks on network they have need to improve on secure network infrastructure [30][27][36] as an example in DETER Project may use modified infrastructure that provide secure facilities, tools and processes for national resource experimentation lab in cyber security[28]. This will ultimately improve the quality of service by accessing altered infrastructure with new web services [34] that may run on different software's [35]. So to continue improve or increase the QOS(quality of service) they have needed to put efforts on security strategies by proposing cyber security education course plan for upcoming generation [20].The objective of this plan is to introduce with the new security websites portal [12] and this next generation technology will may help to detect attacks before launching [1]. Common online security threats are relentlessly inventive because of they find a new way to annoy and steal information as well as resources [31] having many shapes like malware, polymorphic malware strains [37] (i.e. these are used for the detection of unknown attacks) scripts, codes and active contents [43]. Most commonly they will use a method of challenge based learning [13]. The reason to utilize this technique is it will provide a safeguard for storing confidential information in safe manner. To gain control over such types of attacks this will be a biggest challenge [21] for security professionals.

In this paper, authors designed a new private browser named ***"RIM ROCKS"*** whose function is to provide security on the time of client server communication. If any user wants to use this new designed private browser then he or she must be registered. After the confirmation of the registration, user will start browsing from the internet. This new designed methodology **"3SEMCS"** is termed **as Three Step Encryption Method for Cyber Security.** The complete working of this new designed methodology is based on several encryption algorithms. In addition, the major significance to utilize this new designed methodology is it may provide security from phishing websites through passing URL'S from phish tank [58] during client server communication. Presently, security professionals added extensions in the form of options in Google Chrome and Firefox [59], [63] for the detection of phishing sites. This new designed may help to provide online security from the phishers especially on the time of client server communication.

2. REVIEW OF LITERATURE

Seth and Chuchra et al (May-2015), discussed about different types of cyber path hacking attacks on the time of request entered into the search engine during client server communication. Authors designed a methodology "OTBP-Using RRSA" that is termed as an Operational Technology Based procedure-Using Round Robin Scheduling Algorithm" whose complete working is based on unique auto-generated hash address that further provide automatic path encryption when request move towards web server. [44]

Chuchra and Seth et al (Dec-2013), discussed about the recent phishing attacks performed on several bank servers during online money transfer. Such types of attacks are called "On-line Fraud" attacks. Attackers most commonly launch DOS (Denial of Service) and DDOS (Distributed Denial of Service) attacks on bank servers for stealing money online. They used port scanning and online rule-induction data mining technique for identification of phishing attacks. These proposed methodologies may help to analyze the attacker behavior on the time of sending of data from the one point to another. [45]

Chuchra and Mehta et al (April-2013), In this paper, authors integrated two different fields' viz. web mining, network security for the detection of online attacks by utilizing web agents(i.e. - web boots/web robots). Two types of functions were performed by web agents where first function is to detect the type of active attack performed by the attacker and second one is how to provide prevention form such type of specific attack. Authors implemented rule induction based data mining technique for receiving maximum accuracy in results. The collaboration for utilizing hybrid approach is to save time as well as cost where both are the major objectives of the data mining. [46].

3. RESEARCH DESIGN

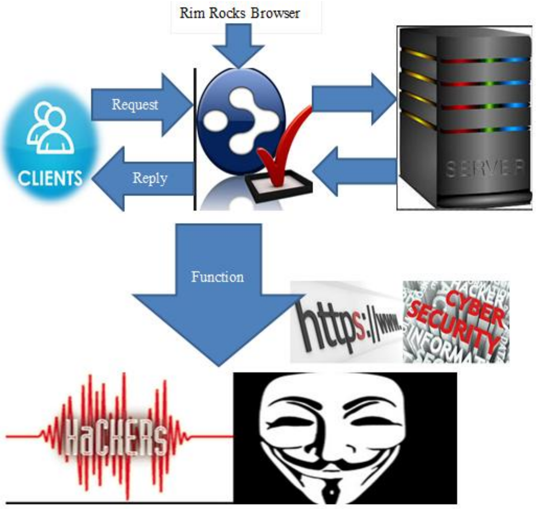


Fig.5: Client Server Communication- Running on RimRocks Brower.

The design of new designed Personnel Browser – ***"RIM-ROCKS"***.

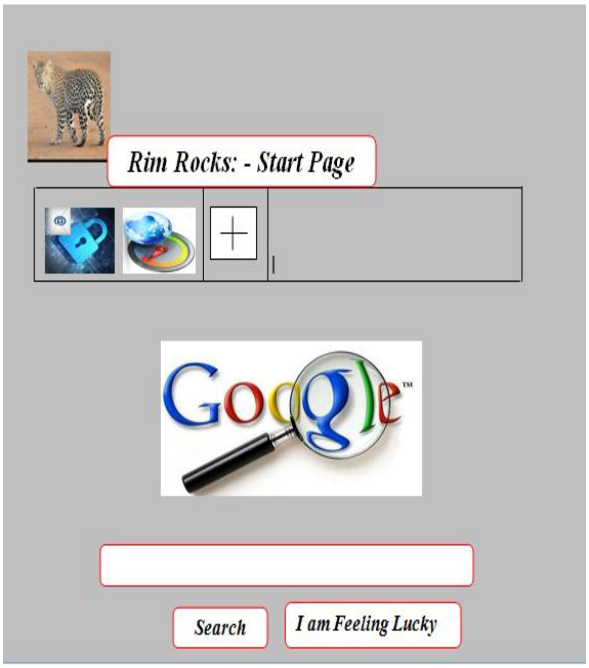
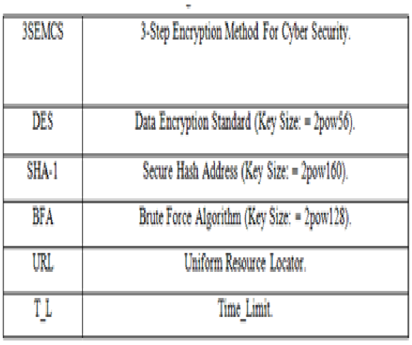


Fig.6: Design of RimRocks Browser.

4. PROPOSED PROCEDURE-3SEMCS

Table.1: Nomenclature for 3SEMCS:



3SEMCS	3-Step Encryption Method For Cyber Security.
DES	Data Encryption Standard (Key Size: = 2pow56).
SHA-1	Secure Hash Address (Key Size: = 2pow160).
BFA	Brute Force Algorithm (Key Size: = 2pow128).
URL	Uniform Resource Locator.
T_L	Time_Limit.

3SEMCS (Browser,Status,Time_Limit, Hash Address, Key Size, Encyrption_Algo (BFA/DES/SHA), Index _Pointer, Google Web Page, URL Address)

Step-1) Design a Personnel Browser.

Step-2) On_Mouse_Click:= Browser_Open and STATUS: = READY TO USE.

Step-3) Confirm Registration. [SET: = User_ID and Pwd: = STRING].

Step-4) When USER SEND REQUEST ON SEARCH ENGINE: = ACCESS FILE FROM WEB THEN Software automatically Generate Encrypted_Hash_Address. In Addition Check the Status of The Website.

```
IF (CHK_URL_WEBSITE:= TRUE)
        {
                Not included In Phish Tank. This website is legitimate or Original.
        }
ELSE
        {
        Website is Fake or affected by Phisher.
        }
```

// Rim Rocks will correspondingly check either the website either it is effected by the phisher or not. Phish Tank help for checking the addresses of different websites.

Step-5) AS REQUEST PROCEED:= Movement_of_Encrypted_Hash_Addess_Start.

Step-6) APPLY ENCRYPTION ALGORITHM: = URL_Of_Web_Page. (DES/SHA). // 2-step encryption is provided.

Step-7) AFTER THAT APPLY CAST-128 bit = On_Already_Encrypted_Hash_Addess* in Step 6. //3-step encryption is provided.

```
Step-8) Set: = Session_Key_On_Already_Encrypted_Hash_Address** of Step 7 THEN CHECK WHETHER THE STATUS_OF_WEB_PAGE.
        IF (T_L = 1 Mintue)
        {
            Index_Pointer:= MOVE NEXT TO CURRENT_STATUS_OF_GOOGLE_PAGE.
        }
ELSE
    {
        Index_Pointer:= 1st Page_of_Google OTHERWISE Repeat step 2 to step 4.
    }
Step-9) IF (Attacker_Send_Request:= Copying_Path_From_URL Address)
        {
THEN Web_Page:= Expire and Generates a Warnning_Message.
        }
    Else
        {
        URL_Addess:= COPIED.
        }
Step-10) END.
```

5. WORKING

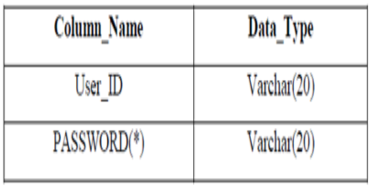
At first step, start from the Sign-Up page from the personnel browser Rim Rocks for confirming the membership through registration. When the user got registered that indicates the account has been successfully created on that private or personnel browser. After the confirmation of registration, user will use that private browser for further secure transactions with the server during information exchange (i.e. or on the time of client server communication). *In the 2nd step*, when user submit own request on search box then at first auto-generated encrypted hash address will be displayed on google page after that when user click on next google page the movement of encrypted hash address will start towards next google page as an example in google page number two. On the time of single mouse click apply strong encryption algorithm as an example DES and SHA-1 for more tighten the security on path that actually provides 2-step encryption towards google page as an example page number three. *In the third step*, further apply brute force algorithm for achieving the top level of security on google page as an example google page number four. *In the fourth step*, set session key on already encrypted hash address**, if the time limit is equal to one then google page index pointer is moved next to current status of google page otherwise google page index pointer again switch into google page number one after that repeat step 2 to 4 correspondingly it may check either the accessed site is effect by the phisher or not?. If the site is not effected by phisher then user request is proceed to next page otherwise Rim Rocks browser display a message of Blocked site – Phishing site is there and ask user do you want to move next if yes then click on yes? *At last step*, if attacker send request for copying the path of URL Address then automatically web page will got expire and generates a warning message alert otherwise URL address of specific path will be easily copied and attacker will easily launch an attack on browser in future on path especially.

6. IMPLEMENTATION

Front-End: .NET FRAMEWORK.

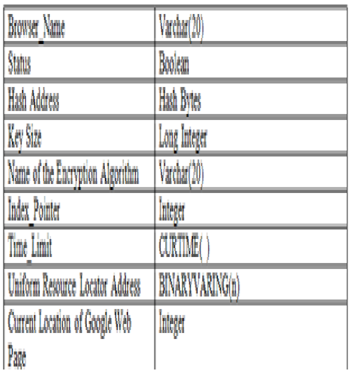
Back-End: SQL SERVER.

Table.2: Personnel Browser Rim Rocks Registration Form



Column_Name	Data_Type
User_ID	Varchar(20)
PASSWORD(*)	Varchar(20)

Table.3: Three Step Encryption Security Mechanism:



Browser_Name	Varchar(20)
Status	Boolean
Hash Address	Hash Bytes
Key Size	Long Integer
Name of the Encryption Algorithm	Varchar(20)
Index_Pointer	Integer
Time_Limit	CURTIME( )
Uniform Resource Locator Address	BINARYVARING(n)
Current Location of Google Web Page	Integer

Step-1)

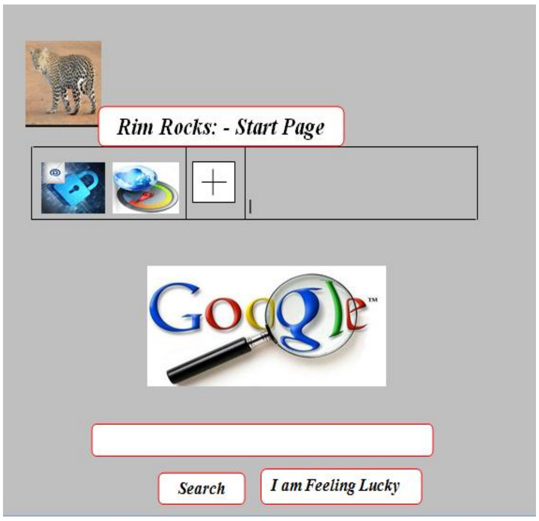


Fig.7: Running of Personnel Browser-RimRocks.

Step-2)

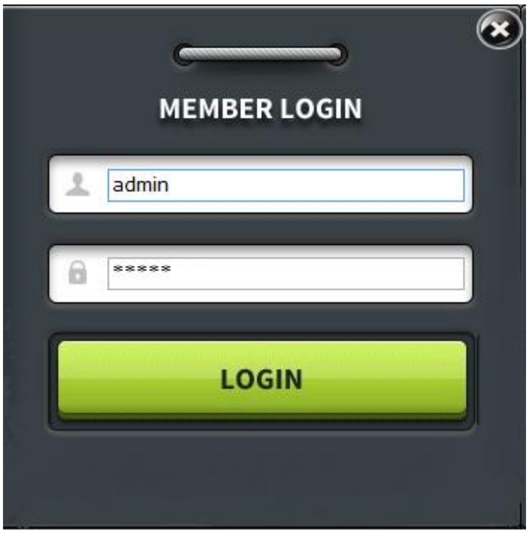


Fig.8: Login for Registration in RimRocks.

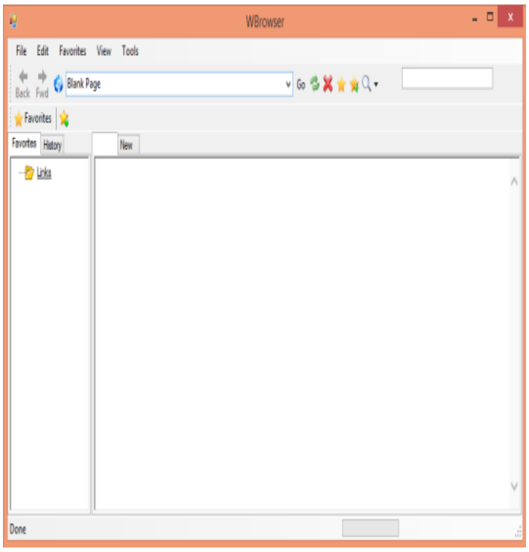
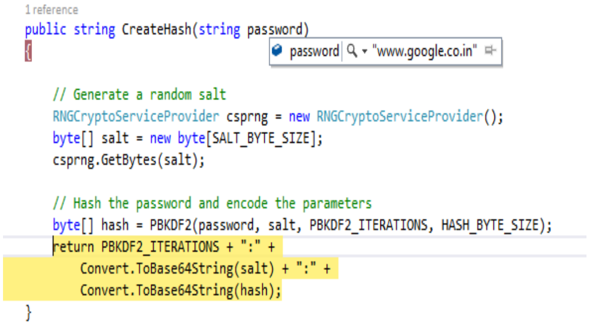


Fig.9: Registration is Confirmed and Browser is Ready to Use.

Step-3)



```
1 reference
public string CreateHash(string password)
{

    // Generate a random salt
    RNGCryptoServiceProvider csprng = new RNGCryptoServiceProvider();
    byte[] salt = new byte[SALT_BYTE_SIZE];
    csprng.GetBytes(salt);

    // Hash the password and encode the parameters
    byte[] hash = PBKDF2(password, salt, PBKDF2_ITERATIONS, HASH_BYTE_SIZE);
    return PBKDF2_ITERATIONS + ":" +
        Convert.ToBase64String(salt) + ":" +
        Convert.ToBase64String(hash);
}
```

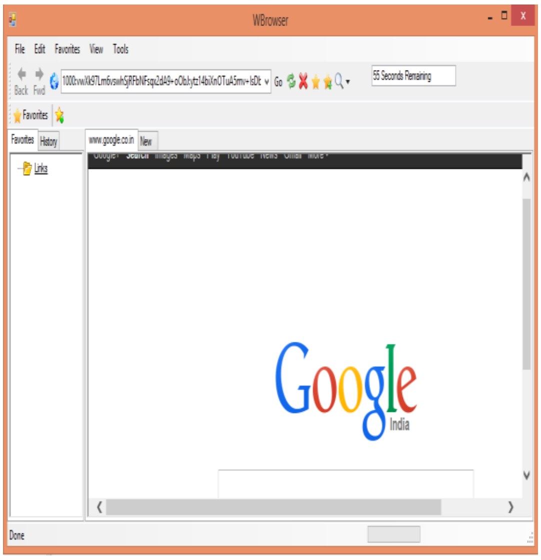
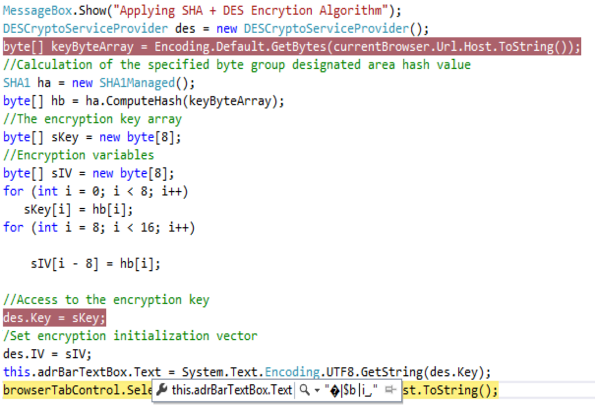


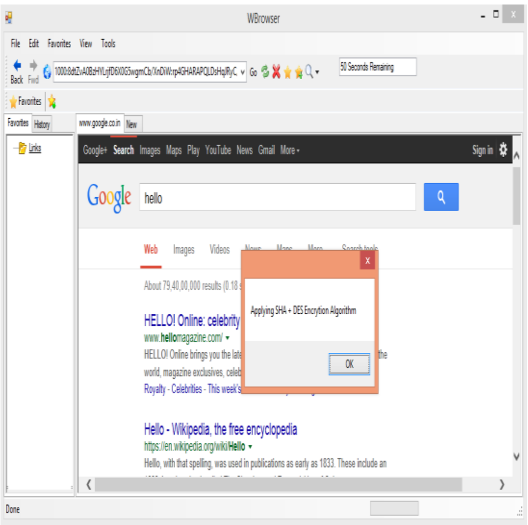
Fig.9: On entering Request of client- Automatically Hash key is generated for providing security.

Step-4)



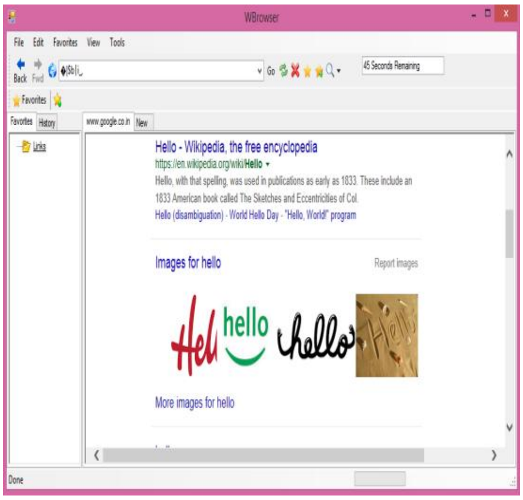
```
MessageBox.Show("Applying SHA + DES Encrytion Algorithm");
DESCryptoServiceProvider des = new DESCryptoServiceProvider();
byte[] keyByteArray = Encoding.Default.GetBytes(currentBrowser.Url.Host.ToString());
//Calculation of the specified byte group designated area hash value
SHA1 ha = new SHA1Managed();
byte[] hb = ha.ComputeHash(keyByteArray);
//The encryption key array
byte[] sKey = new byte[8];
//Encryption variables
byte[] sIV = new byte[8];
for (int i = 0; i < 8; i++)
   sKey[i] = hb[i];
for (int i = 8; i < 16; i++)

    sIV[i - 8] = hb[i];

//Access to the encryption key
des.Key = sKey;
/Set encryption initialization vector
des.IV = sIV;
this.adrBarTextBox.Text = System.Text.Encoding.UTF8.GetString(des.Key);
browserTabControl.Sele                                  st.ToString();
```

this.adrBarTextBox.Text "�|$b|i_"


WBrowser
File Edit Favorites View Tools
Back Fwd
Go
50 Seconds Remaining
Favorites
History
Links
www.google.co.in
New
Google+ Search Images Maps Play YouTube News Gmail More
Sign in
Google
hello
Web Images Videos
HELLO! Online: celebrity
Hello - Wikipedia, the free encyclopedia
Done

Applying SHA + DES Encryption Algorithm

OK



Hello - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Hello
Hello, with that spelling, was used in publications as early as 1833. These include an 1833 American book called The Sketches and Eccentricities of Col.
Hello (disambiguation) - World Hello Day - "Hello, World!" program

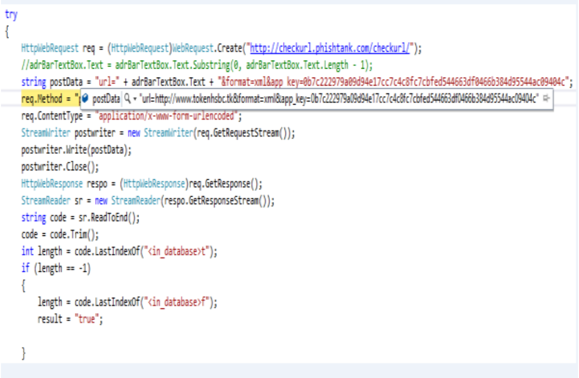
Images for hello Report images

More images for hello

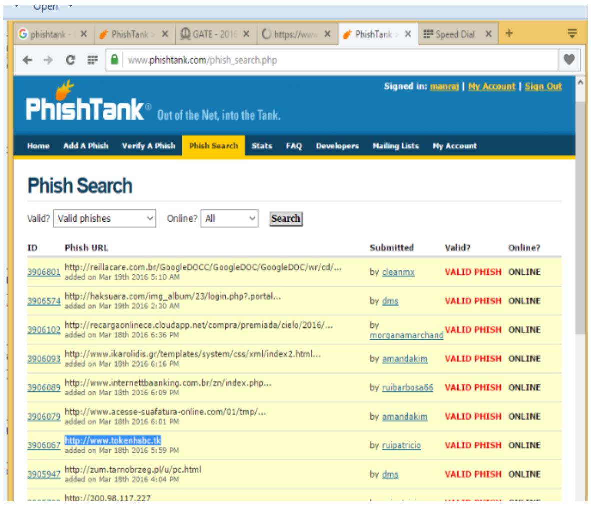
Fig.10: Two-Step Encryption [SHA + DES]is Applied**

```
IF (CHK_URL_WEBSITE:= TRUE)
        {
            Not included In Phish Tank. This website is legitimate or Original.
        }
    ELSE
        {
        Website is Fake or affected by Phisher.
        }
```

// Rim Rocks will correspondingly check either the website either it is effected by the phisher or not. Phish Tank help for checking the addresses of different websites.



```
try
{
    HttpWebRequest req = (HttpWebRequest)WebRequest.Create("http://checkurl.phishtank.com/checkurl/");
    //adrBarTextBox.Text = adrBarTextBox.Text.Substring(0, adrBarTextBox.Text.Length - 1);
    string postData = "url=" + adrBarTextBox.Text + "&format=xml&app key=0b7c222979a09d94e17cc7c4c8fc7cbfed544663df0466b384d95544ac09404c";
    req.Method = "p postData "url=http://www.tokenhsbc.tk&format=xml&app_key=0b7c222979a09d94e17cc7c4c8fc7cbfed544663df0466b384d95544ac09404c"
    req.ContentType = "application/x-www-form-urlencoded";
    StreamWriter postwriter = new StreamWriter(req.GetRequestStream());
    postwriter.Write(postData);
    postwriter.Close();
    HttpWebResponse respo = (HttpWebResponse)req.GetResponse();
    StreamReader sr = new StreamReader(respo.GetResponseStream());
    string code = sr.ReadToEnd();
    code = code.Trim();
    int length = code.LastIndexOf("<in_database>t");
    if (length == -1)
    {
        length = code.LastIndexOf("<in_database>f");
        result = "true";

    }
```



www.phishtank.com/phish_search.php

Phish Search

ID	Phish URL	Submitted	Valid?	Online?
3906801	http://reillacare.com.br/GoogleDOCC/GoogleDOC/GoogleDOC/wr/cd/... added on Mar 19th 2016 5:10 AM	by cleanmx	VALID PHISH	ONLINE
3906574	http://haksuara.com/img_album/23/login.php?.portal... added on Mar 19th 2016 2:30 AM	by dms	VALID PHISH	ONLINE
3906102	http://recargaonlinece.cloudapp.net/compra/premiada/cielo/2016/... added on Mar 18th 2016 6:36 PM	by morganamarchand	VALID PHISH	ONLINE
3906093	http://www.ikarolidis.gr/templates/system/css/xml/index2.html... added on Mar 18th 2016 6:16 PM	by amandakim	VALID PHISH	ONLINE
3906089	http://www.internettbaanking.com.br/zn/index.php... added on Mar 18th 2016 6:09 PM	by ruibarbosa66	VALID PHISH	ONLINE
3906079	http://www.acesse-suafatura-online.com/01/tmp/... added on Mar 18th 2016 6:01 PM	by amandakim	VALID PHISH	ONLINE
3906067	http://www.tokenhsbc.tk added on Mar 18th 2016 5:59 PM	by ruipatricio	VALID PHISH	ONLINE
3905947	http://zum.tarnobrzeg.pl/u/pc.html added on Mar 18th 2016 4:04 PM	by dms	VALID PHISH	ONLINE
	http://200.98.117.227			

Fig.11: Legtimated Sites URL will checked through Phish Tank.

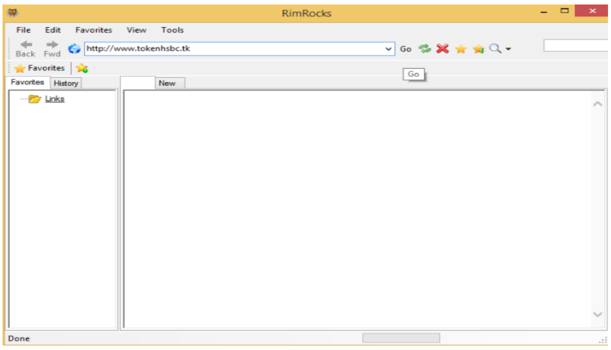
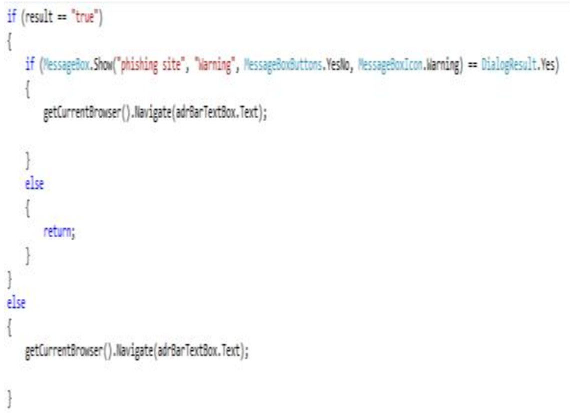


Fig.12: Website is Orignal: URL does not exists in Phish Tank.



```
if (result == "true")
{
    if (MessageBox.Show("phishing site", "Warning", MessageBoxButtons.YesNo, MessageBoxIcon.Warning) == DialogResult.Yes)
    {
        getCurrentBrowser().Navigate(adrBarTextBox.Text);

    }
    else
    {
        return;
    }
}
else
{
    getCurrentBrowser().Navigate(adrBarTextBox.Text);

}
```

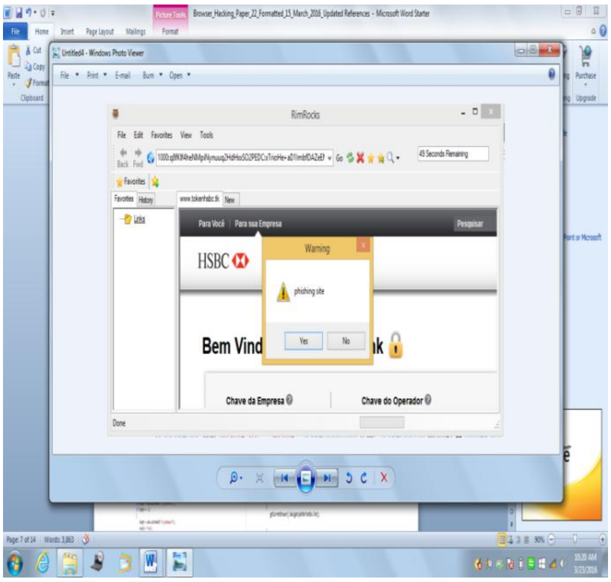
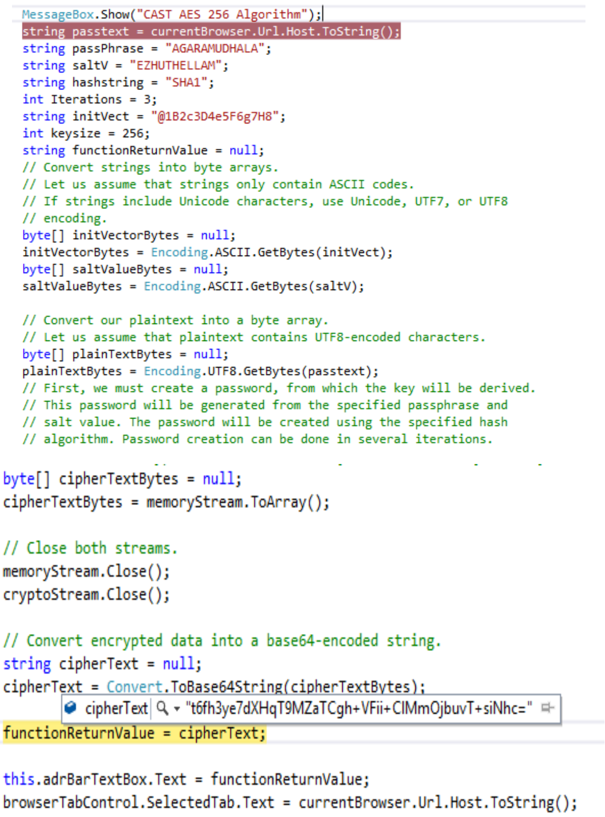
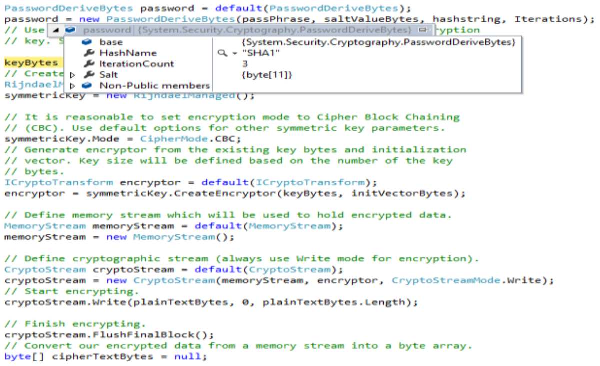


Fig.13: Website is Fake(Phished Website) : Because of URL exists in Phish Tank.

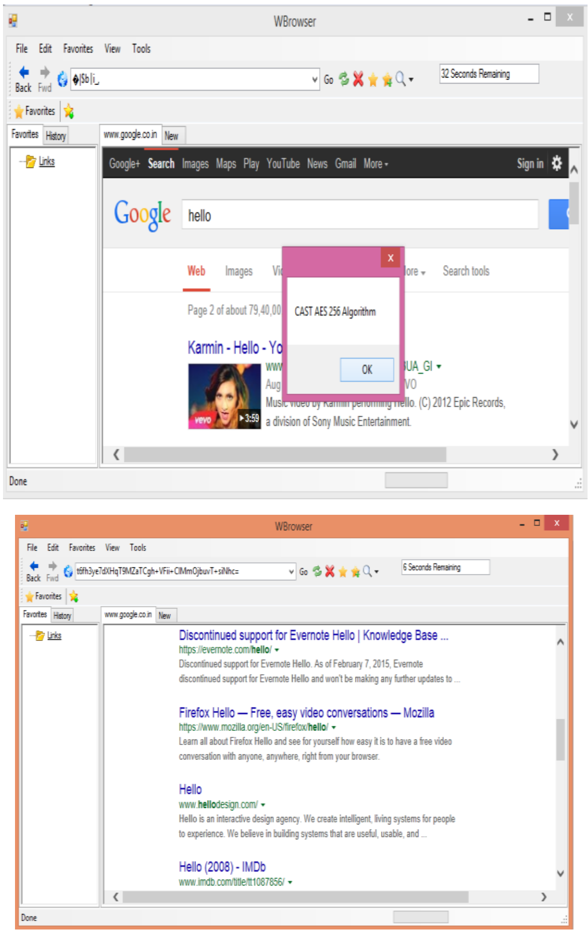
Step-5)



```
MessageBox.Show("CAST AES 256 Algorithm");
string passtext = currentBrowser.Url.Host.ToString();
string passPhrase = "AGARAMUDHALA";
string saltV = "EZHUTHELLAM";
string hashstring = "SHA1";
int Iterations = 3;
string initVect = "@1B2c3D4e5F6g7H8";
int keysize = 256;
string functionReturnValue = null;
// Convert strings into byte arrays.
// Let us assume that strings only contain ASCII codes.
// If strings include Unicode characters, use Unicode, UTF7, or UTF8
// encoding.
byte[] initVectorBytes = null;
initVectorBytes = Encoding.ASCII.GetBytes(initVect);
byte[] saltValueBytes = null;
saltValueBytes = Encoding.ASCII.GetBytes(saltV);

// Convert our plaintext into a byte array.
// Let us assume that plaintext contains UTF8-encoded characters.
byte[] plainTextBytes = null;
plainTextBytes = Encoding.UTF8.GetBytes(passtext);
// First, we must create a password, from which the key will be derived.
// This password will be generated from the specified passphrase and
// salt value. The password will be created using the specified hash
// algorithm. Password creation can be done in several iterations.

byte[] cipherTextBytes = null;
cipherTextBytes = memoryStream.ToArray();

// Close both streams.
memoryStream.Close();
cryptoStream.Close();

// Convert encrypted data into a base64-encoded string.
string cipherText = null;
cipherText = Convert.ToBase64String(cipherTextBytes);
    cipherText | "t6fh3ye7dXHqT9MZaTCgh+VFii+CIMmOjbuvT+siNhc="
functionReturnValue = cipherText;

this.adrBarTextBox.Text = functionReturnValue;
browserTabControl.SelectedTab.Text = currentBrowser.Url.Host.ToString();
```



```
PasswordDeriveBytes password = default(PasswordDeriveBytes);
password = new PasswordDeriveBytes(passPhrase, saltValueBytes, hashstring, Iterations);
// Use   password | {System.Security.Cryptography.PasswordDeriveBytes}   ryption
// key. S   base                 {System.Security.Cryptography.PasswordDeriveBytes}
            HashName             "SHA1"
keyBytes    IterationCount       3
// Create   Salt                 {byte[11]}
RijndaelM   Non-Public members
symmetricKey = new RijndaelManaged();

// It is reasonable to set encryption mode to Cipher Block Chaining
// (CBC). Use default options for other symmetric key parameters.
symmetricKey.Mode = CipherMode.CBC;
// Generate encryptor from the existing key bytes and initialization
// vector. Key size will be defined based on the number of the key
// bytes.
ICryptoTransform encryptor = default(ICryptoTransform);
encryptor = symmetricKey.CreateEncryptor(keyBytes, initVectorBytes);

// Define memory stream which will be used to hold encrypted data.
MemoryStream memoryStream = default(MemoryStream);
memoryStream = new MemoryStream();

// Define cryptographic stream (always use Write mode for encryption).
CryptoStream cryptoStream = default(CryptoStream);
cryptoStream = new CryptoStream(memoryStream, encryptor, CryptoStreamMode.Write);
// Start encrypting.
cryptoStream.Write(plainTextBytes, 0, plainTextBytes.Length);

// Finish encrypting.
cryptoStream.FlushFinalBlock();
// Convert our encrypted data from a memory stream into a byte array.
byte[] cipherTextBytes = null;
```



CAST AES 256 Algorithm

OK

Music video by Karmin performing Hello. (C) 2012 Epic Records, a division of Sony Music Entertainment.

t6fh3ye7dXHqT9MZaTCgh+VFii+ClMmOjbuvT+siNhc=

Discontinued support for Evernote Hello | Knowledge Base ...
https://evernote.com/hello/
Discontinued support for Evernote Hello. As of February 7, 2015, Evernote discontinued support for Evernote Hello and won't be making any further updates to ...

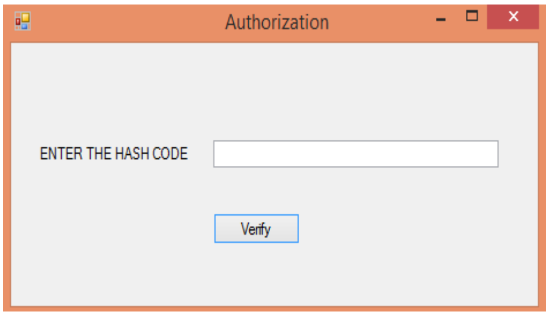
Firefox Hello — Free, easy video conversations — Mozilla
https://www.mozilla.org/en-US/firefox/hello/
Learn all about Firefox Hello and see for yourself how easy it is to have a free video conversation with anyone, anywhere, right from your browser.

Hello
www.hellodesign.com/
Hello is an interactive design agency. We create intelligent, living systems for people to experience. We believe in building systems that are useful, usable, and ...

Hello (2008) - IMDb
www.imdb.com/title/tt1087856/

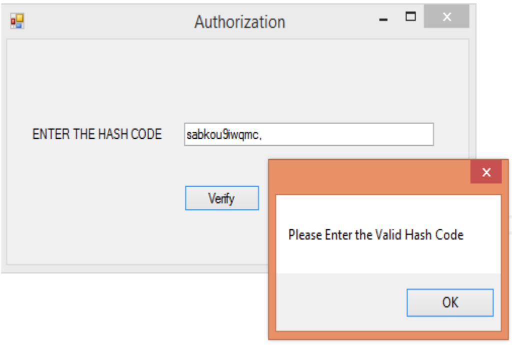
Fig.14: Three-Step Encryption is Applied(DES+SHA+CAST Encrption Algorithm).

Step-6)



ENTER THE HASH CODE

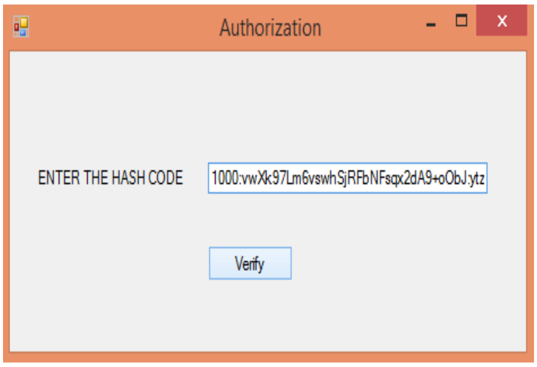
Fig.15: Enter Hash Code for the confirmation of authorized User before expiring session.



ENTER THE HASH CODE sabkou9iwqmc,

Please Enter the Valid Hash Code

Fig.16: Wrong hash key submitted by Unauthorised user(Hacker).



ENTER THE HASH CODE 1000:vwXk97Lm6vswhSjRFbNFsqx2dA9+oObJ:ytz

Fig.17: Verification of Hash Code.

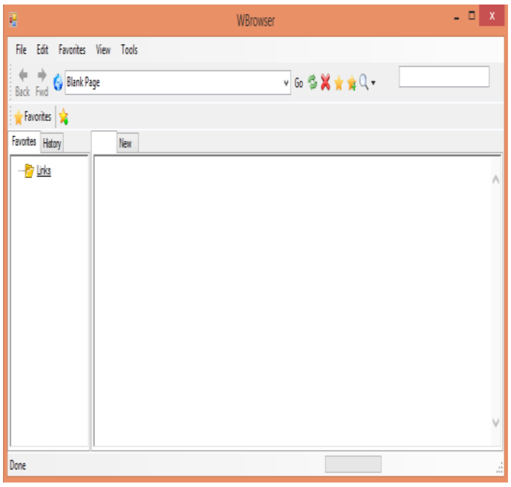
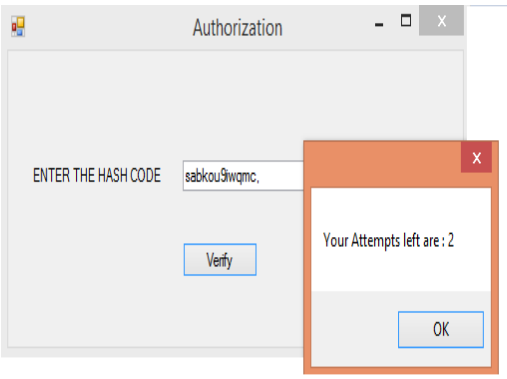


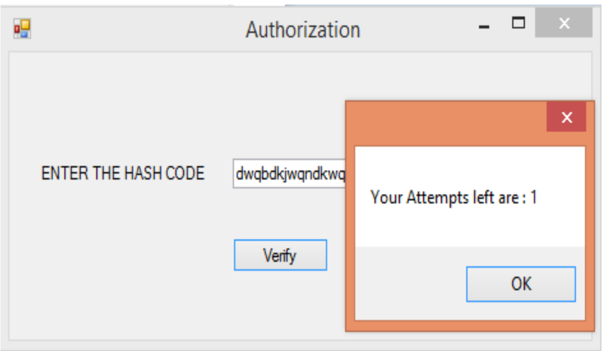
Fig.18: Hash code Verified.



ENTER THE HASH CODE sabkou9iwqmc,

Your Attempts left are : 2

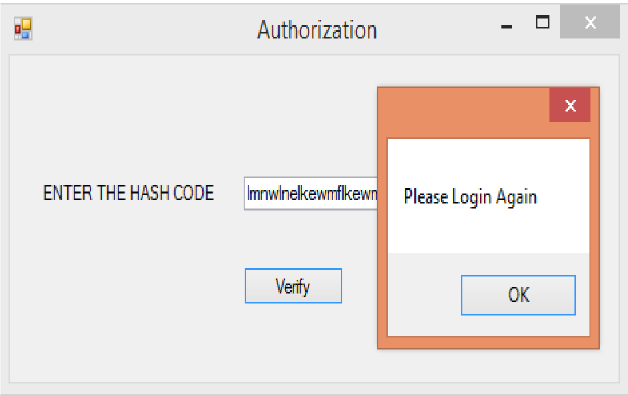
Fig.19: User will try for entering correct code maximum 2 times.



ENTER THE HASH CODE dwqbdkjwqndkwq

Your Attempts left are : 1

Fig.20: User will try for entering correct code maximum 1 time.



ENTER THE HASH CODE lmnwlnelkewmflkewn

Please Login Again

Fig.21: Entered code is incorrect: Warnning message Alert.

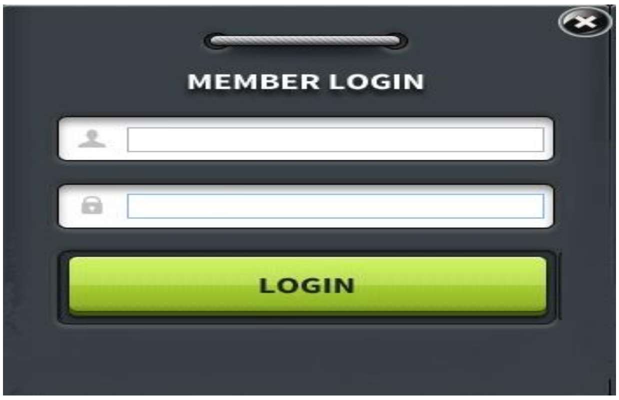


Fig.22: Login Again in RimRocks.

7. RESULTS AND DISCUSSIONS

According to the results calculated by the authors they said this new designed three step encryption methodology helps us to achieve a highest level of security during client server communication. Suppose if any unauthorized user may want to gain access then he or she may take some time as an example at least one minute to perform any attack. If attacker entered wrong hash key after session expires then need to login once again. If attacker entered valid session key then browsing continues. For reducing the attacks, author's uses this new designed methodology that may help to reduce especially phishing attacks in future. In this way, this new designed private browser named "Rim Rocks" helps to enhance online security.

8. CONCLUSIONS

A variety of cyber hacking attacks have been reviewed and analyzed in this paper. Such types of attacks may considerably be reduced by developing this methodology ***3SEMCS*** that is termed as a Three-Step Encryption Method for Cyber Security. This proposed methodology will run on new designed private browser that is named as “Rim Rocks”. The complete working of this proposed procedure is based on auto-generated encrypted hash address where the movement of encrypted hash address towards next google page shows ***two-step encryption**** on the path by utilizing strong encryption algorithms like DES and SHA-1. On the next move on google page this will further provide encryption up to ***third highest level on path***** for more tighten the security by utilizing brute force algorithm. In addition, this designed methodology may help to provide security from the phishers. The study of three step encryption method is actually enhance the potential of upcoming encryption technologies and its implifications to defense and government users. In this way, authors say the use of new designed private browser provides a more secure channel of communication during information exchange on the time of client server communication.

9. FUTURE SCOPE

This work will be extended by utilizing WIRESHARK Tool on private browser named as Rim Rocks. The purpose to utilize this WIRESHARK Tool is to provide real time monitoring of data on the network. By implementing different algorithms WIRESHARK will provide prior warning message alerts that help to prevent from hackers & correspondingly gives the complete information of the network as like what is exactly going on the network as like the time of enter and exit of hacker from the network.

10. REFERENCES

[1] Sr.Analyst,,Sr.Chiranshu Ahuja and Atul Kumar. Cyber Security Research Developments, DSCI (Promoting Data Protection).

[2] Privacy and Cyber Security-Emphasizing Privacy Protection in Cyber Security Activities, December-2014.

[3] Geneva, A Comparative Analysis of Cyber Security Initiatives Worldwide, International Telecommunication Union.

[4] Michal Bailey and Erin Kenneally, Cyber Security Research Ethics Dialogue and Stategy Workshop, CCR Online, USA.

[5] Emergance of Cyber Security Law, Febuary-2015. Prepared for the Indiana University Maurer School of Law by Hanover Research, Indiana University Bloomington.

[6] Developing our capability in cyber security, Academic Centers of Excellence in Cyber Security Research, HM Government.

[7] Rossouw von Solms and Noluxolo Kortjan, July -2014.A conceptual framework for cyber-security awareness and education in SA, School of ICT, South Africa.

[8] Robert Menshaw,2012.NSA initiatives in Cyber Security Science-The Next Wave.

[9] Aaron Burstein, Conducting Cyber Security Research Legally and Ethically, School of Law, University of California.

[10] Sanjay Rai, 2014. Cyber Security - IIARF Research Report, The institute of Internal Auditors Research Foundation.

[11] David Whyte, D’Arcy Walsh and Dan Craigen,July-2013.Securing Canada’s Information Technology Infrastructure: Context, Principles and focus areas of Cyber Security Research.

[12] Eduard Hovey and David Kepler, A Taxonomy and a knowledge portal for cyber security, US.

[13] Fabio Elia, Henry Z.Lo,Joseph P Chen,Ronald S.cheung, Challenge Based Learning in Cyber Security Education ,University of Massachusetts,USA.

[14] Rita Tehan,2014.Cyber Security: - Authoritative Reports and Resources by topic, Federal Publications, Digital Commons, ILR, Corell University.

[15] www.rewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/.

[16] First Cluster Workshop on Cyber Security in FP7 Security & Trust Research Projects-Report,Co=Organized with CYSPA.//www.cspforum.eu/member-states.

[17] Tobby Simon & Michal Chertoff, Febuary-2015. The Impact of the dark web on Internet Governance & Cyber Security, Global Commission on internet governance.

[18] Cybconf2015.am.gdynia.p1/CYBERSEC.

[19] Marco Spruit and Tjalling Reijmer, March-2014.Cyber Security in the news-Technical Report, Netherland.

[20] Sara Sinclair and Michael E.Locasto,2009.An experience Report on Undergraduate Cyber-Security Education & Outreach, ACEIS,USA.

[21] www.diplomacy.edu/cybersecurity.

[22] G.J.U Gander Reddy and G.Nikhita Reddy,A Study of Cyber Security Challenges and its emerging trends on latest Technologies”, Osmania University, Hyderabad, India.

[23] Deanna D.Caputo and Shari Lawrence Pfleeger,2012.Leveraging Behavioral Science to Mitigate Cyber Security Risk”, MITRE Corporation.

[24] Dr. George and A Wright, Cyber Security: Designing and Maintaining Resilience, Georgia Technical Research Institute of Cyber Technology and information, Security Laboratory.

[25] Pankaj Kumar Kesetewani, Abhishek Vaish and Aniruddha Singh, January-2014. Information Security: Components and techniques.

[26] Dipankar Dasgupta,Yunyue Lin,Denise Ferebee and Qishi Wu,An Integrated Cyber Security Monitoring System Using Co-relation Based Techniques, University of Memphis.

[27] Sachin Goyal,Ratish Aggarwal and Raghav Gupta,April-2014. A Review of Cyber Security Techniques for critical Infrastructure Protection,International Journal of Computer Science and Engg. Technology.

[28] Terry Benzel, The Science of Cyber Security Experimentation the DETER Project,USC Information Science Institute.

[29] Adil Yousif,Adil Ali A. Alaziz,Othman Ibrahim,Nadir Omer Fadl Elessied,2011,Review-Paper: Security in E-Government Using Fuzzy Methods,International Journal of Advanced Science and technology.

[30] RH Goudar,Bina Kotiyal and Priti Saxena,April-2012.A Cyber Era Approach for Building Awareness in Cyber Security For Educational System in India ,International of information and education technology.

[31] Ateeq Ahmad,Type of Security Threats and its prevention, International Journal of Computer Technology and Applications.

[32] Kadoleayashi Youki and Takahashi Takeshi, Cyber Security Information Exchange Techniques: Cyber Security Information Ontology and CYBEX.

[33] Salvatore Stolfo, Ramawamy Devarajan and Brian Bowen, Measuring the human factor of cyber security, Columbia University.

[34] John Suffolk, Oct-2013.Cyber Security Prospectives:- Making Cyber Security a part of Companies, DNA-A set of integrated Processes, Polices and Standards, Huawei Technologies.

[35] Tamara G.Kolda and Daniel M.Dunlavy and Bruce Hendrickson, Feb-2009.Mathematical Challenges in Cyber Security,Sandia Laboratory-Unlimited Release,California.

[36] Yasuko Fukuzawa,Kunihiko Miyazaki,Makoto Kayashima and Satoshi Takemoto,2014.Trends in Cyber Security and Latest Countermeasures, Hitachi Review.

[37] Iulian Neamtiu and Tudor Dumitras, Experimental Challenges in Cyber Security: A story of Provenance and Lineage for Malware -white paper, University of California.

[38] Research Report on IBM Security Services 2014:- Analysis of Cyber Attack and incident data from IBM's Worldwide security operations, IBM Global Technology Services.

[39] Vinod Kumar Sharma and Himanshu Gupta,Augst-2013.Multiphase Encryption:- A new concept in Modern Cryptography, International Journal of Computer Theory and Engg.

[40] Tommie Singleton,October-2013.The top 5 Cyber Crime, American Institute of CPA'S.

[41] Lockheed Martin Corporation and Mical Muckin and Scott C.Fitch,A Threat-Driven approach to cyber security, Lockheed Martin Co-orporation.

[42] Pekka Vepsalainen and Angeliki Tsocholl, 2014. "Strategic Research Agenda for Cyber Trust,DIGLE.

[43] Ramlan Mahmoud,Ali Dehgantanha and Mohsen Damshenas,2013. A survey on Malware Propoagation,analysis and Detection,International journal of cyber security and digital Forensis.

[44] R.K Seth, Rimmy and Shubham Chuchra, May-2015, Proposing Operational Technology based procedure (OTBP) Using Round Robin Scheduling Algorithm, International Journal of Computer Applications.

[45] Rimmy Chuchra and R.K Seth, December-2013. On the mechanism of detection and Prevention from Phishing Attacks By Analyzing Attacker Behavior ,International Journal of Advanced Research in Computer Science and Software Engg.

[46] Rimmy Chuchra and Bharti Mehta, April-2013.Use of Web Mining in Network Security, International Journal of Emerging Technology and Advanced Engg.

[47] Kruegel Christopher & Kirda Engin,Protecting users against phishing attacks with Antiphish,White paper, Technical University of Vienna.

[48] Reddy Madhusudaan V.C, Safar Vidya.U,October-2013.Intelligent phishing website detection and prevention system by using link guard algorithm,Journal of Computer engineering.

[49] N.Banu Shaira and Mohideen Mohammed,Febuary-2014.Email Phishing-An open threat toi everyone,International Journal of scientific & research publications.

[50] Cranston Christopher,Anti-Phishing as a web based user service,University of Strachlyde,UK.

[51] Salleh Mazleenaa and Zeydan Zuhair Hiba, December-2014.Current state of anti-phishing approaches and revealing competencies, Journal of Theoretical and applied information technology.

[52] Cranor Lorrie and Hong Jason,2007.CANTINA-A Content based approach to detecting phishing web sites, International world wide web conference committee,Canada.

[53] Wu.M and R.Miller,April-2006.Do security toolbars actually prevent phishing attacks?, In proceedings of ACM Conference on Human Factors in computing systems.

[54] Khan Khalid Muhammad and Memon Khan Imraan, March-2013.Anti-Phishing for mid-range mobile phones, International Journal of computer and communication engineering.

[55] Wolman Alec, Saroin Stefan and Ronda Troy, iTrust Page: A User assisted anti-phishing tool, UK.

[56] Abhyankar Asmita and Rewadkar.N.D, 2014.A Reviews of anti-phishing Framework based on visual cryptography, International journal of science and research.

[57] Kruegel Christopher and Kirda Engine,On the effectiveness of techniques to detect phishing sites, Technical university Vienna.

[58] Shukla Kumar and Piyush,2015.System Design-Investigation and Countermeasure of Phishing Attacks using Data Mining Classification Methods and Its Analysis. International Journal of Advanced Science and Technology.

[59] Wang HAINING AND Yue Chauan, Anti-Phishing is offence & defense. The college of William and Marry.

[60] B.Vani Maddhura and M.Reddy,September-2013. A novel anti-phishing framework Based on Visual Cryptography, International Journal in Computer and Communication.

[61] Baj.S,Divekar Vishal and Malwade Ashutosh,March-2014. An enhanced anti-phishing framework based on visual cryptography, International journal of emerging research in management and technology.

[62] Sarje.K Anil and Oberoi Kapil,An anti-phishing application for end user.

[63] Xin Yang and Ouyang Xi, April-2012.An empirical analysis of the effectiveness of browser based anti-phishing solutions, International Journal of digital content technology and its applications.

[64] Mishra Varsha ,June-2014.A survey of various anti-phishing techniques, Universe of emerging technologies and science.

[65] Punjyaban Patel and Deeply Dubey,December-2015. Secured Techniques of anti-phishing in cryptography: A Review., International Journal of innovative research in computer and communication engg.

[66] Schmitz Poland and Li Shujan, 2009.A Novel Anti-Phishing Framework based on HoneyPots,Proceedings of fourth annual APWG ecrime researchers summit(ECRS),IEEE.

[67] Lee Ju Isug and Ku-Heng Ching, Building a frame based anti-phishing model based on phishing ontology.

[68] Tabasco Alexdendra and Luner Ion,2010.OPptimizing anti-phishing solutions based on user awareness, education and the use of latest web security solutions, Informatics Economica.