Modeling Implementation of TSEA - Three Step Encryption Algorithm for Enhancing Password Security

Rimmy Chuchra
Department of Computer Science & Engg
Sri Sai College of Engg. And Technology,
Manawala (Amritsar)

R.K. Seth
Department of Applied Sciences
Sri Sai University
HP (India)

ABSTRACT
Cryptography is an art of secret writing that provides protection from unauthorized access. This paper discusses about the several databases attacks and proposes a new methodology for enhancing password security during Sign-In of account. This designed methodology is termed as "three step encryption algorithm (TSEA)" whose function is to provide a high level of security on the time of accessing account. The complete working of this designed methodology is based on automatic hash address generation. The main focus of this paper is to improve the overall quality of service for right person at a right time in a procedural manner.

Keywords
Hash Code, Text Encryption, encryption algorithm, Image Encryption, Security, Databases Attacks

1. INTRODUCTION
Cyber world is going to become more popular day by day because of the growth of internet users become increases. Most of the tasks are handled with the help of internet in the form of transactions as an example ticket reservation, online shopping and internet banking etc. For handling such type of hard real time transactions, security professionals has need to organize confidential information in such a way so that any third party that either may be a hacker or any unauthorized user will not access that confidential data. So, to provide prevention of data from unauthorized users they may use different types of encryption algorithms as an example DES [2] [3] [4] [14] and SHA-512[4, 18] that provide a secure channel during communication. The primary duty of security professionals is deep analysis of data that is to be carried on the wire and in the next step they decide the types of strategies are to be implemented for specific one. For achieving top level of security most of the security professionals uses several encryption algorithms [1] that consider key size is important factor. For providing tight security like security procedures implemented in banks they most commonly uses the concept of session key whose function is change value automatically when session will be expire [17] that may help to reduce the chances of attack up to some extent. As authors did survey on different types of security attacks they found in results most of the times attackers target the systems through databases attacks by utilizing several methods or techniques on the network as an example privilege escalation, unnecessary database service alerts and they mostly prefer to steal back-ups from unencrypted tapes [21] etc. And some other attacks are SQL Injection, Insider attack, Network attacks and Trojan horses etc that can be discussed below:

1.1 SQL Injection
The input field is modified in such a way that the database itself returns unintended data. It's main function is to concatenate the fixed part of SQL statement with user-supplied data that can be easily shown in the form of some additional sub-queries on the database as an example any attacker comes and insert a series of SQL statements into a ' query' that may further help us to manipulate the data input. In general, attacker may use two different types of SQL injections' viz. Normal SQL injection, Blind SQL Injection that can be discussed below with the help of an example:

1.1.1 Normal SQL Injection
Attacker directly adds Structured Query language code to a Web form input box to gain access of resources or make changes in data that can be shown in fig.1.1.1:

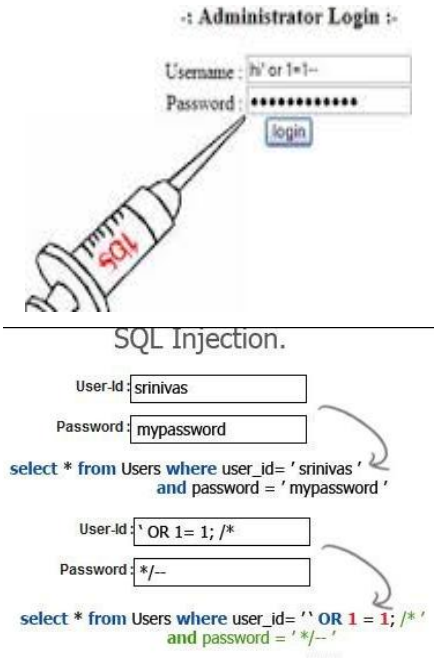


Fig 1.1.1. Normal SQL Injection: Applied directly on databases [12] [13]

Query Representation of Normal SQL Injection can be shown below with the help of SQL example:

a. www.example.org/display.php?item=**1** (**Actual** query).

b. www.example.org/display.php?item=**1'** (Injected Query).

1.1.2 Blind SQL Injection
In this case, Attacker tries to make many combinations of attacks that additionally give the complete information regarding the attempt of next attack. It is based on the interpretation of resulting html page output of previous page that can be discussed below:

a. http://victim/showproduct.asp?id=238 and 1=1.

b. http://victim/showproduct.asp?id=238 and 1=2.

The URL'S (Uniform Resource Locator) of a & b queries may show the same results of two different queries [22].

Where the results of blind SQL injection may be same or different that depends. These two separate types of injections having two major differences that are listed below:

a) Method of retrieving data from the databases is different.

b) Normal SQL Injection is concerned with error message where Blind SQL Injection is not.

1.2 Insider Thread

By applying insider thread, attackers leaked information electronically simply that can be shown in fig.1.2:

Fig 1.2. Insider threads [23] [24]

Such kind of attacks can be handled by limiting the number of users with specific level of access.

1.3 Network attacks

Such types of attacks are more concerned with web servers that additionally gives access to the database as an example denial of service attack. Mostly, it performs on banking sites for stealing money that may be in the form of online-fraud attack that can be shown in fig.1.3:

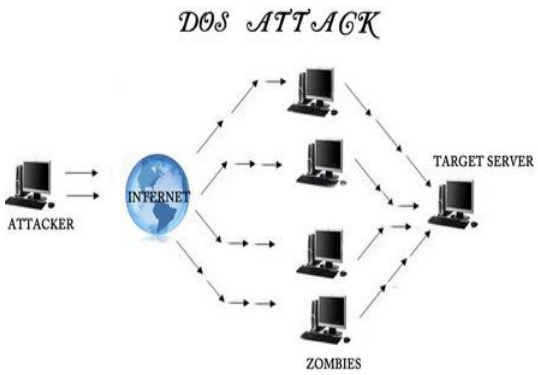


Fig 1.3. Denial of Service attack [25].

1.4 Trojan Horses

It's purpose is to corrupt various software applications that helps to leak confidential information that can be shown in fig.1.4:

Fig 1.4. Effect of Trojan horse Attack [26] [27]

The function of Trojan horse is to modify the copy and then send sensitive information to unauthorized locations or users that may in future utilize by unauthorized user for performing some additional illegal changes.

Such types of attacks in future may convert into cybercrimes that depends on the behavior of the attacker who is actually a criminal. To provide prevention from databases attacks most commonly security professionals uses two methods viz. IDS (Intrusion detection system) and use various security measures for database servers. The goal of IDS is to find out the different flavors' of suspicious traffic in different ways. The use of IDS is to provide system and network monitoring. It's the duty of database administrator to provide prevention from IDS by using further two methods viz. encryption on firewalls and security on IP addresses that can be discussed below:

- By using encryption on DB Firewalls: Apply encryption on firewalls that may help to provide a periodic check for several database configurations as well as settings.
- By providing security on IP Addresses: Domain name server (DNS) who save the list of registered IP Addresses, if any request will be coming from outside that is to be considered as illegal IP Address or request coming from the attacker server (i.e. specific IP Address was not registered on DNS) then it will be automatically blocked or discarded by the server and at last it displays a warning message alert.[28]

By implementing these two above discussed security methods database security will be easily enhanced.

The objective of this paper is to enhance the password security which is stored on the database and provides a better quality of service during Sign-in. This paper proposes three step encryption algorithm (TSEA) whose function is to provide a high level of security on the password when fetched from the databases during sign-in. The complete working of this designed methodology is only depend on the auto-generated hash address. This auto-generated hash address is further considered as a key for the next step of TSEA. Authors contribute their efforts for providing encryption on text that results image encryption and provide a highest level of security while utilizing designed methodology. The steps of designed methodology named TSEA are given below:

Table.1: Nomenclature for TSEA:

SRC ADD	Source Address.
DEST ADD	Destination Address.
KSIZE	Key Size.
REF	Run Encryption Function.

Step-1) INITIALIZE: = [SRC ADD, DEST ADD, KSIZE]. After that RUN ENCRYPTION FUNCTION.

Step-2) CREATE NEW FILE for DES THEN SAVE ALL DATA exists in Specific Image.

Step-3) FILE INCLUDE: = DES ARRAY [N] and SHA ARRAY [N] algorithm. // N is number of elements exists in Array.

Step-4) RUN FILE = RECEIVED ENCRYPTED IMAGE // Final Output.

Step-5) Exit

The formula used by authors for designed methodology for providing 3 step encryption can be described in table.2:

HCE+SIE → FIE.

Table.2: Different Types of Encryption used in TESA:

HCE	Hash Code Encryption
SIE	Selected Image Encryption
FIE	Final Image Encryption

Even there are different types of techniques are used by the security professionals for enhancing image security [13]. Most commonly they use CHAOS image encryption[5,20] method [11,12] because of it provides a higher level of security[15] by considering time and speed factors and that can be shown in fig.1.5:

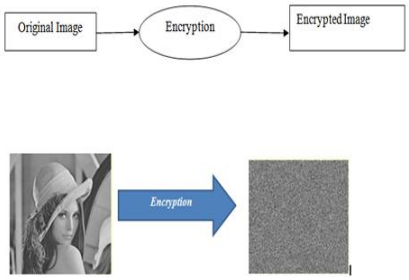
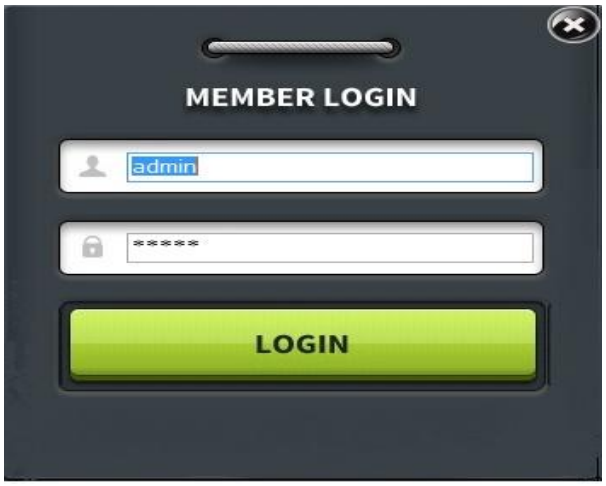


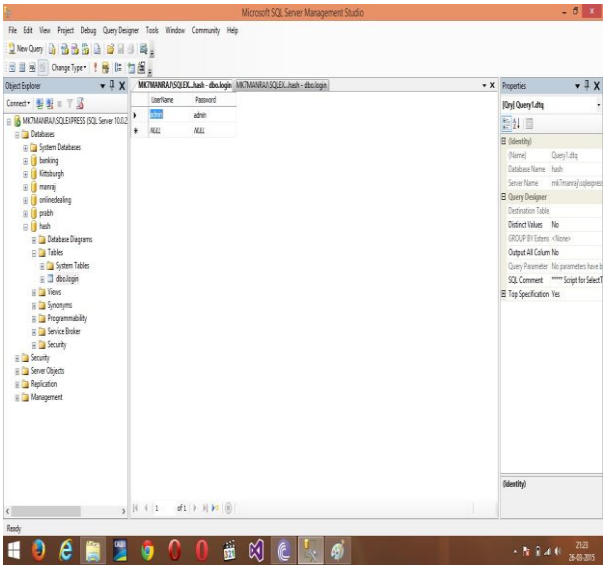
Fig.1.5. Image Encryption[9]

Where the general classification of image encryption can be categorized into two group's viz. position permutation based algorithm [6], value transformation based algorithm [7, 8]. Digital image is a collection of the pixels with different intensity values [16] and that also provides an ease of scrambling of images that correspondingly decrease the correlation among the pixels [5]. The working of designed methodology is totally depends on text encryption that results in the form of image encryption [5] where image encryption facilitate us about the highest percentage of the multi-media data [10, 19]. In this way, authors concluded image encryption is more secure or powerful than text encryption.

2. IMPLEMENTATION OF TSEA

Step 1) SET U_ID:= String & PWD: = string THEN Click on LOG_IN & access account.



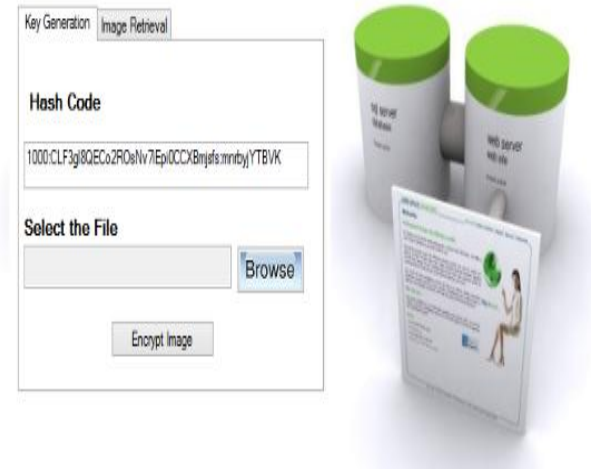


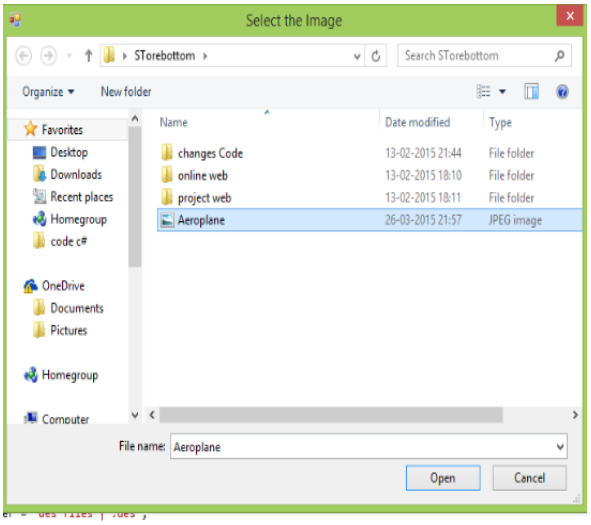
Step 2) IF (U_ID & PWD = CORRECT)

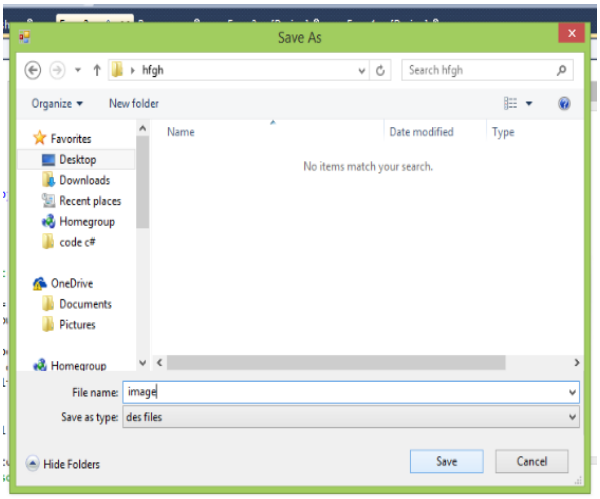
{

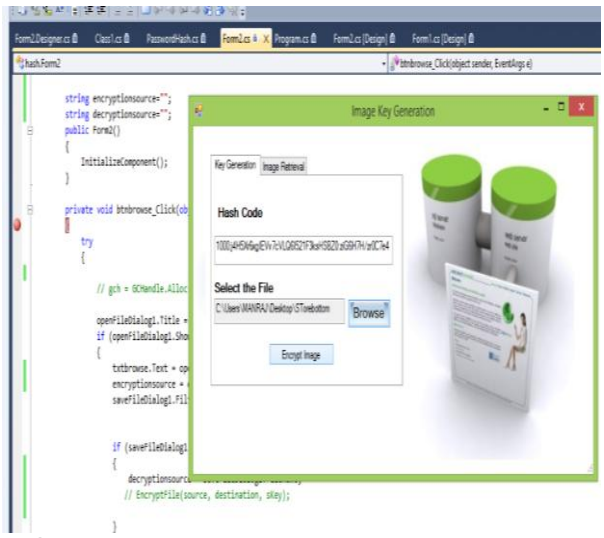
Hash Add: = Auto-generated & mapped with D_IMG at specified Location.

}









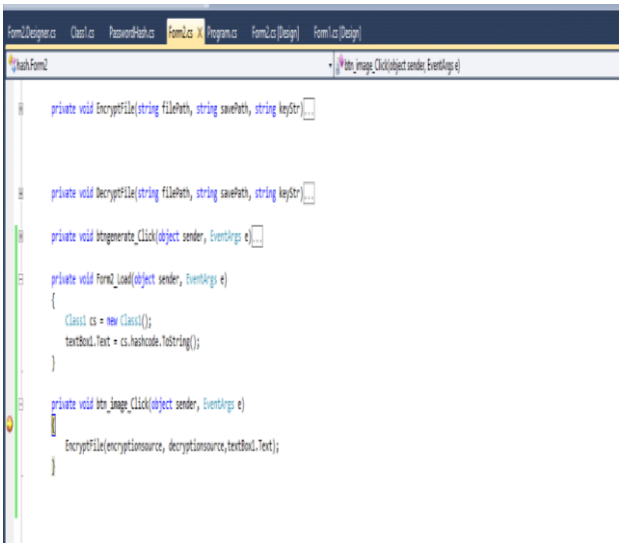
ELSE

{

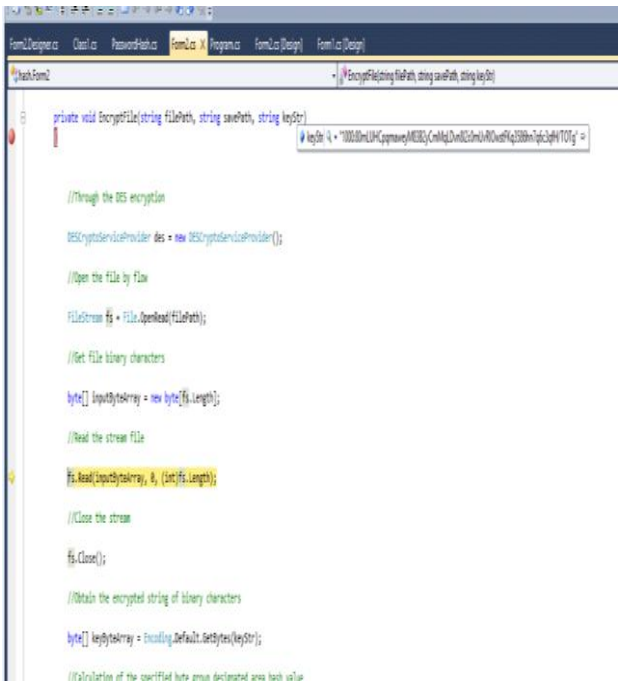
Invalid LOG_IN (Move to step 1).

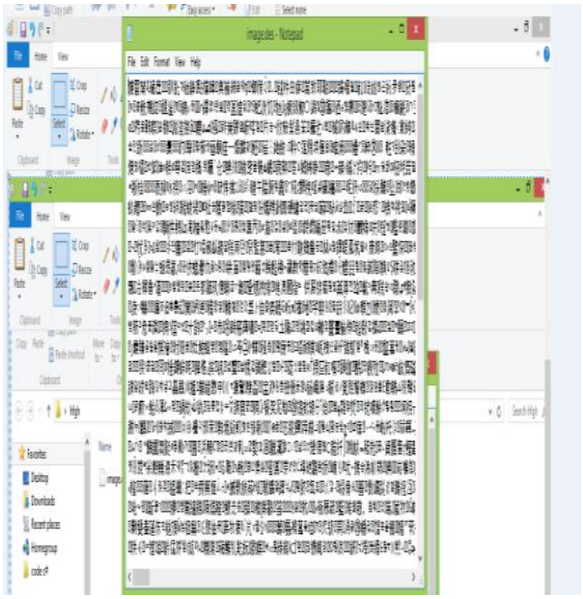
}

Step3) THEN U_APPLY:= ENCYPTION_ON_HASH_CODE.



Step-4)ENCRYPTED_HASH_CODE= IMAGE_ENCRYPTION.





Step 5) Exit

3. WORKING

At first user enter a string for Id and password for accessing any account. When user click on Log_In button then verifies that specific id and password, is it match with database entries or not? If user id is not matched then sign_in again otherwise user confirms own authentication and after that move to second step, software automatically generates a unique hash address that already mapped with the digital image that is placed in specific location on the system. The digital image is browsed by the user. In the third step, user applies automatic-encryption on auto-generated hash address at first and then applies encryption on mapped image. At last step, DES and SHA collectively results in the form of image encryption.

4. CONCLUSION

Different types of database attacks are reviewed and analyzed. Several databases attacks may considerably be reduced by developing the procedure as designed in this paper. The complete working of this designed methodology is based on the auto-generated hash address. At last, text encryption results image encryption. In this way, this designed methodology may help for enhancing the database security during accessing of an account and provides better quality of service.

5. FUTURE SCOPE

In future the strength of security during sign_in will be enhanced by providing session based encryption algorithm. This proposed methodology may help to reduce the chances of attacks on databases especially on the time of sign_in. The time spent by the specific client after sign_in on another page is important factor.

6. REFERENCES

[1] Harivan Partap Singh, Shweta Verma, Shailendra Mishra, feb 2013. Secure Data Encryption Algorithm", International journal of advanced research in electrical electronics and instrumentation Engg.

[2] Debajit Sensarma,Samar Sen Sarina, March 2014,GMDES-A Graph based modified data encryption Standard(DES) Algorithm with Enhanced Security ,International journal of research in engg and technology.

[3] National Institute of Standards, 1977, FIPS 47: DES, US.

[4] Amit Keswani & Vaishnava Khadilkar, The SHA-1 Algorithm, USA.

[5] Rinki Pakshwar,Vijay Kumar Trivedi,Vineet Richhariya, 2013. A Survey on Different Image encryption & Decryption Techniques, International Journal of Computer Science and Information Technology.

[6] Juin-In Guo,Jui-Cheng Yen,2000. A New Mirror Like Image Decryption Algorithm &bits VLSI Architecture pattern recognition and image analysis, International Journal of Computer Science and Information Technology.

[7] Aloha Sinha and, Kehar Singh, A Technique for image encryption using Digital Signature, Optics Communications.

[8] S.S Mani Ccam, N.O Bourbackis, 2001. Lossless Image Compression & Encryption Algorithm Using SCAN, Pattern Recognition.

[9] Rajinder KAUR,Er.Kawalprit,March-April 2014,Image Encryption Technique: A Selected Review ,IOSR Journal of Computer Engg(IOSR-JCE).

[10] Abinav Srivastva,2012. A Survey Report on Different Techniques of Image Encryption, International Journal of emerging Technology & Advanced Engg.

[11] Ephin M, Judy Ann Joy and N.A Vasanthi, 2013, Survey of chasos based image encryption & decryption technique, International Journal of Computer Applications, Proceedings on Amrita International Conference of women in computing.

[12] Sukalyan Som,Sayani Sen,2013.A Non-Adaptive partial encryption of Crrayscale Images base on Chaos ,First international conference on computational Intelligence: Modeling Techniques & Applications(CIMA),ELSEVIER.

[13] Sonam Pathak and RACHNA Kamble,july-2013.A Review: Chaotic System with DES Image Encryption Technique, International Journal of Advanced Research,

IT Bhopal.

[14] P.Radhadevi, P.Kalpna,oct-2012. Secure Image Encryption Using AES, International Journal of research in Engg. And Technology.

[15] Nan Lin,Xiaofeng Guo,Ping Xu and Yuqin Wang,2013.A New Multi-Chaos based Image Encryption Algorithm, Intelligence Computation & Evolutionary Computation Advances in Intelligent Systems & Computing.

[16] Mohammad Sajid , Proff. S.T Bodka and Qamurddin Khizari,june-july-2013. Image encryption using different techniques for high security Transmission over a Network, International Journal of engg research & General Science.

[17] Shruthi K.S, G.Padmaja Devi and P.C Srikanth, Aug-2014.Secured Text and Image Encryption based on session, International Journal of industrial Electronics and Electrical Engg.

[18] Abbas Cheddad,Joan Condell, Kevin Curran and Paul Mukevitt,March-2010. A Hah based image encryption algorithm, Optics Communications-ELSEVIER.

[19] Nitin .N,Ankumar M.Bangale,G.P hedge,oct-2012. Image encryption based on FEAL Algorithm , International Journal of advances in computer science & Technology.

[20] Chengqing li, Guanrong Chen, On the security of a class of image encryption schemes, SAR,China.

[21] http://www.darkreading.com/risk/hackers-choice-top-six-database-attacks/d/d-id/1129481?

[22] Special Issue on the data mining for information security2013. ELSEVIER-Information sciences.

[23] https://www.google.co.in/search?q=image+for+insider+thread&tbm=isch&tbo=u&source=univ&sa=X&ei=DAupU9jsAYaiugT_pIG4CQ&ved=0CBwQsAQ&biw=1024&bih=639#facrc=_&imgdii=_&imgrc=NBJEacXm7KxYMM%253A%3BXh_XssbqO8R1gM%3Bhttp%253A%252F%252Fwww.executivegov.com%252Fwpcontent%252Fuploads%252F2011%252F03%252Finsiderthreat.jpg%3Bhttp%253A%252F%252Fwww.executivegov.com%252F2011%252F03%252Fintel-observers-see-wikileaks-chilling-effect-on-information-sharing%252Finsider threat%252F%3B448%3B299.

[24] https://www.google.co.in/search?q=image+for+insider+thread&tbm=isch&tbo=u&source=univ&sa=X&ei=DAupU9jsAYaiugT_pIG4CQ&ved=0CBwQsAQ&biw=1024&bih=639#facrc=_&imgdii=_&imgrc=QMhjid6iSYm1aM%253A%3B1pNS_4NTspq0pM%3Bhttp%253A%252F%252Fstatic.itpro.co.uk%252Fsites%252Fitpro%252Ffiles%252Fstyles%252Fgallery_wide%252Fpublic%252Fimages%252Fdir_163%252Fit_photo_81883.jpg%253Fitok%253Du_ykpt3u%3Bhttp%253A%252F%252Fwww.itpro.co.uk%252F614326%252Fbusinesses-should-focus-on-the-accidental-insider-threat%3B940%3B627

[25] https://www.google.co.in/search?hl=en&site=imghp&tbm=isch&source=hp&biw=1024&bih=639&q=image+for+insider+thread+for+database+attack&oq=image+for+insider+thread+for+database+attack&gs_l=img.3...1658.9779.0.10000.44.15.0.29.1.1.217.1796.0j11j1.12.0....0...1ac.1.48.img..33.11.1566.dojcSRJTWpU#hl=en&q=image+for+denial+of+service&tbm=isch&facrc=_&imgdii=_&imgrc=0s0nqXX0xq4GM%253A%3BmZ54S9qKKYET3M%3Bhttp%253A%252F%252F2.bp.blogspot.com%252FomtiQZZ2Z1w%252FTrJdQP8sfEI%252FAAAAAAAAAAPU%252F7qvomdiQf60%252Fs1600%252Fdos%252Battack.jpg%3Bhttp%253A%252F%252Feffecthacking.blogspot.com%252F2011%252F11%252Fdenial-of-service attack.html%3B1600%3B1000.

[26] https://www.google.co.in/search?hl=en&site=imghp&tbm=isch&source=hp&biw=1024&bih=639&q=image+for+insider+thread+for+database+attack&oq=image+for+insider+thread+for+database+attack&gs_l=img.3...1658.9779.0.10000.44.15.0.29.1.1.217.1796.0j11j1.12.0....0...1ac.1.48.img..33.11.1566.dojcSRJTWpU#hl=en&q=image+for+TROJAN+HORSES&tbm=isch&facrc=_&imgdii=_&imgrc=cUkl2JEK07AXKM%253A%3BO6lGE0h9hBGw1M%3Bhttp%253A%252F%252Fwww.friendlycomputerssouthhouston.com%252Fwpcontent%252Fuploads%252F2010%252F12%252Ftrojanhorse.gif%3Bhttp%253A%252F%252Fwww.friendlycomputerssouthhouston.com%252Ftrojan-horses-adware-and spyware%2525E2%252580%252594what%2525E2%252580%252599s-the difference%252F%3B551%3B413.

[27] https://www.google.co.in/search?hl=en&site=imghp&tbm=isch&source=hp&biw=1024&bih=639&q=image+for+insider+thread+for+database+attack&oq=image+for+insider+thread+for+database+attack&gs_l=img.3...1658.9779.0.10000.44.15.0.29.1.1.217.1796.0j11j1.12.0....0...1ac.1.48.img..33.11.1566.dojcSRJTWpU#hl=en&q=image+for+TROJAN+HORSES&tbm=isch&facrc=_&imgdii=_&imgrc=9S32F7_ULIuRZM%253A%3B1brKEYiZygRcNM%3Bhttp%253A%252F%252Fnews.techgenie.com%252Ffiles%252FTrojanHorse.png%3Bhttp%253A%252F%252Fnews.techgenie.com%252Flatest%252Fhow-trojan-horses-work%252F%3B532%3B438

[28] M.M Chaturvedi & Preeti Aggarwal, Oct-2013. Application of data mining techniques for information security in a cloud: A Survey, International journal of computer application.