PERCEIVE AND PREVENT DATA OOZE USING LSB EMBEDDING

[1]Srishti Vasekar, [2]Prof. Aaradhana Deshmukh
[1]PG Student, GTU PG School, Gandhinagar, Gujarat, India
[2]Ass. Professor, Department of Computer engineering, Kashibai Navale College of Engineering, Pune, India

Abstract - In the recent business state, an organization has huge challenge that is data ooze. The sensitive information from different organizations consist of Information of person, Intellectual property (IP), credit-card, financial data and other sensitive data related to business. This information is shared among different consumers, industry partners, stakeholders etc. This causes the danger of being data leak to unauthorized people and responsible to business image exploitation.
Data ooze is basically leakage in data communication. In our proposed system, it deals with to detect the data ooze and prevent. A Sender sends GIF Image with hiding data to Receiver. During communication there is a chance that Image is leaked. We are focusing on External threat of data ooze. Firewall is used by trusted third party auditor for prevention purpose. LSB embedding is used to hide data in animated gif image. Trusted third party auditor is person who is authorized and monitors the communication channel, detects and prevents the data ooze.

Keywords: Data Ooze, Detection, Prevention, Firewall, LSB Embedding

I. INTRODUCTION

Communication world increasing data usage and transaction is run time exchanges, so during this detect data ooze or leak is big challenge in front of researchers.

The data is sent from the sender to receiver are confidential and secure. It should not be disclosed to any third person who is not authorized. There are lots of sensitive data may include information of person, financial data, credit card information, confidential data, intellectual property, Customer data, other information related to business. Each company has data which is the most important assets. The data leakage may cause serious threats for company. Data is shared among various stakeholders, customers, business partners, etc. This causes the risk of being data leaked to unauthorized users.

Data ooze is basically leakage in data. Data is main assets for every organization. If during communication data is reached at unauthorized person or in some way it leaks that impact on organization and reduces its goodwill and reputation. When data is leaked during a communication among users that is called data ooze problem. Data ooze is distribution of sensitive data either intentional or accidental to the unauthorized persons or by breaking the security rules, policies etc. from outside users who tries to hack information. To protect data from being misused by unauthorized person, it is critical task for business.

Our goal is to detect and prevent the data ooze.LSB Embedding is steganography technique, which employed to embed or replace data into a variety of digital media. If the data which is send by Sender to Receiver is found in a public/private domain then to detect and prevent leakage is a nontrivial task. So, we have trusted third party auditor who monitor the communication channel each and every data which is transmitted. Our main work is as TPA to detect data ooze which happened by external entity and prevent from it. Firewall is system which protects our system from unauthorized access. Firewall is used for preventing purpose by TPA. LSB Embedding is used for hiding data in Animated GIF Image.

II. DATA OOZE DETECTION

Data ooze is basically leakage in data communication. Data ooze poses a critical issue to organizations since there is an increase in data 1oss incidents. There are mainly two types of Data ooze threats: Internal and External.

The Internal threats are caused by authorized employees who perform unauthorized action. Actions are either intentionally or unintentionally which leads to degradation of services or theft of data. Intentional data leakage occurs by the internal user due to unauthorized outsourcing of data and information purposely. Unintentional data leakage occurs by mistake when the authorized users send any sensitive information to outsiders or to any malicious recipient. For example, an employee of an organization sending an email to person who is unauthorized by unintentionally attaching any confidential information. It occurs due to carelessness of Employee.

External threats occur by breaking the security rules, policies from outside users. Outside user who tries to hack the confidential information of an individual or an organization. It mostly occurs due to the following reasons: Data theft by intruders, Malware, Dumpster driving, Phishing, SQL injection and attacks are some type of external threats. In our appraisal the threat for data ooze is external entity. An attacker is entity which attack on system and who is threat of data ooze.

Data theft happens when someone try to get your data illegally. These peoples are often known as attacker/hacker and their goal is to damage or destroy your information or place it on internet for everyone to use. There are mainly two types of attack: Active and Passive attack. In passive attack intruder eavesdrops but does not modify the message stream in any way. In active attack is intruder may transmit messages, replay old messages, and modify messages in transit and man in the middle attack.

III. DATA OOZE PREVENTION

Data leakage prevention is a strategy of preventing the data leakage. Some of the mechanisms that are involved in prevention of data leakage are as follows:

Access Control and Encryption enables to prevent the unauthorized users from accessing the data. Data access control methods like read, write or/and modify techniques can be provided to data for avoiding data being hacked by unauthorized users.

Standard Protection Methods make use of various methods like antivirus, firewall, intrusion detection and prevention systems etc for preventing data from leakage to unauthorized users.

Designated DLP Systems able to identify and control the transfer of sensitive information to other systems. This DLP systems has ability to restrict the copying or transferring of sensitive confidential information to unauthorized users.

Intelligent Security Measures provides techniques for identifying anomalous retrieval of data stored in databases. It is also involved in identify unsecure transfer of email between persons, activity based verification and using honey pot techniques for finding the unauthorized intruders[11].

IV. LSB EMBEDDING

Steganography is practice of undetectably communicating a message in cover object. Steganography use text, audio, video, and image as cover object. Spatial domain/Image domain and Transform domain/Frequency domain are two types of Steganography. Spatial domain deals with the pixels of Image. LSB Substitution technique is an example of spatial domain technique. In transform domain, secret data is embedded into cover after transforming into frequency domain. Discrete cosine transformation technique (DCT), Fast Fourier transformation technique (FFT) and Discrete Wavelet transformation technique (DWT) are various transformation techniques.

The LSB embedding is for embedded large amounts of data without observable changes. In case of image steganography following terms are used Secrete data, Image used to hide secrete data that is Cover image, image with secrete data hided beneath Steganographed image. In which LSB planes is manipulated by directly replacing LSBs of cover-image with the bits of message. LSB methods accomplish high capacity of hiding, accuracy, quality of steganographed image.

There are different method DCT, DWT and LSB. Comparison of these three methods is shown in below table.

Table 1: Comparison of Methods

Method	**DCT**	**DWT**	**LSB**
Capacity of hiding	Average	Good	Good
Accuracy	Average	Good	Good
Embedding and Extraction Technique	Predefined	Can be changed and varying	Predefined
Quality of Steganographed Image	Average	Good	Better
Quality of Extracted Image	Average	Good	Good

LSB embedding is performed on the least significant bit(s). This minimizes the variation in colors that the embedding creates.LSB affects the smallest changes of the 8 bits therefore it alters the image to minimum. The most common method used is called LSB mechanism that is hiding the data object in the LSB of the message. The other techniques include Filtering and Masking. This is normally associated with JPEG.Human eye appear the original image and the final embedded image as identical as shown below figure.

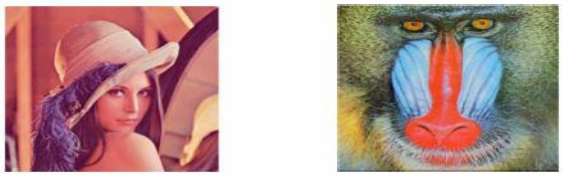

Figure 1: Original Image without LSB[22]

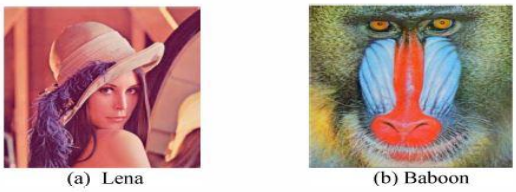

Figure 2: Image with data hide using LSB[22]

V. PROPOSED MODEL

Data ooze is basically leakage of data. Data ooze problem means data is leakage during the communication between sender and receiver. We have to first detect leakage then prevent it. In our proposed system there are mainly four actors i.e. Sender, Receiver, Attacker and Trusted Third Party Auditor.

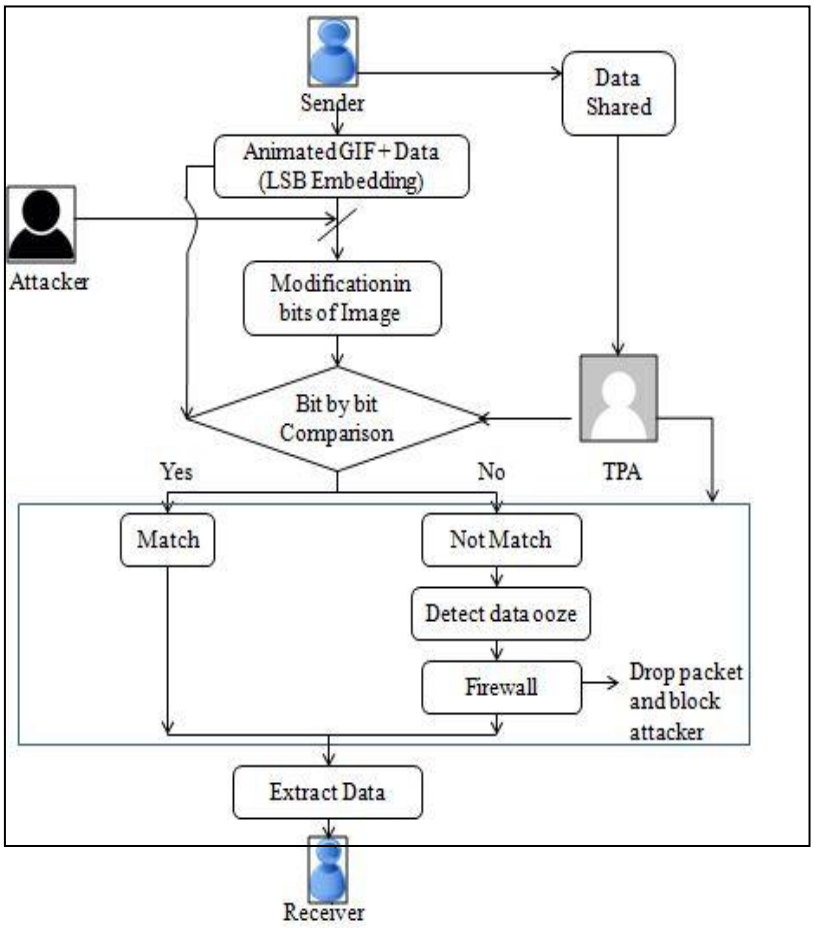

Figure 3. Flow of Proposed System

In our proposed system, the idea is to find efficient and robust system to detect the data ooze. We are focusing on External threat. Figure 3 is show flow of system. Sender first embed data into Animated GIF Image using LSB Embedding. Sender send Embedded Image to Receiver. Before it reaches to the Receiver if the Attacker attacks on system. After attacking image which is in communication channel that having some different bits than original. After attacking by attacker on image the bits of original image is changed. Trusted Third Party Auditor (TPA) which do comparison bit by bit between original image and image which is tamper by Attacker. Goal of attacker is damage or destroy your information. Each and every image is passed through TPA in our system. Database is shared between Sender and Trusted Third Party Auditor which has all the details of Receiver and image which send by Sender. Trusted Third Party Auditor checks each and every image which is send by Sender. So, during bit by bit comparison if it is match then it send to the Receiver there is no problem in GIF Image. But, if bit by bit comparison is not match then at that point Trusted Third Party Auditor detect that data ooze is happened that's why Attacker can able to attack on image.

Then TPA use Firewall. A Firewall can drop a packet that it determines to be malicious and block all further traffic from that IP address or port. So, Here we are use Firewall to drop that packet (GIF Image) which is tampered by Attacker and block that attacker. TPA is an entity which facilitates interactions between sender and receiver who both trust the third party. He reviews all operation, transaction, communication between sender and receiver. The relying parties use this trust to secure their own communications. For Example CA that is Certificate Authority who issues a digital identity certificates issuance.

Now after detection and prevention Trusted Third Party Auditor forward data to Receiver. Image is extracted by Receiver to get original data. After doing LSB Embedding in image there is no observable changes in image.

VI. IMPLEMENTATION

In VMWARE we create 4 ubuntu machine is created.

1. Sender
2. Attacker
3. TPA
4. Receiver

For Data sharing purpose we use ssh server. It is used for passwordless acess services. So that TPA Trusted Third Party Auditor can access data from Sender.

Sender hide data in animated GIF image and send as shown in Figure 4.Here the image is send in blockwise.

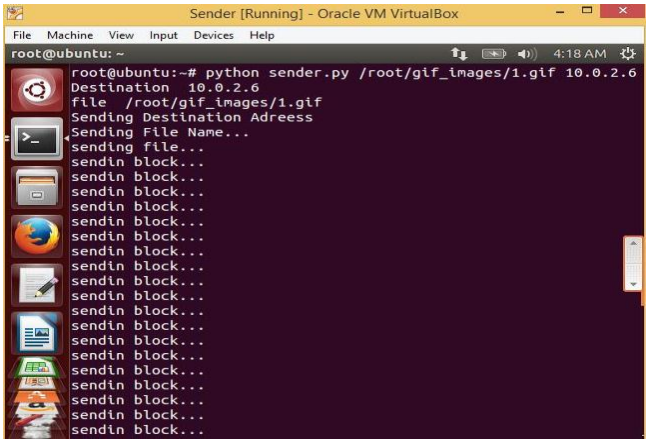

Figure 4 Sender send Animated GIF image

For Attacking purpose Ettercap tool is used. We use MIMA Man in Middel Attack as shown in Figure 5. Using Ettercap Attacker capture data as shown in Figure 6.

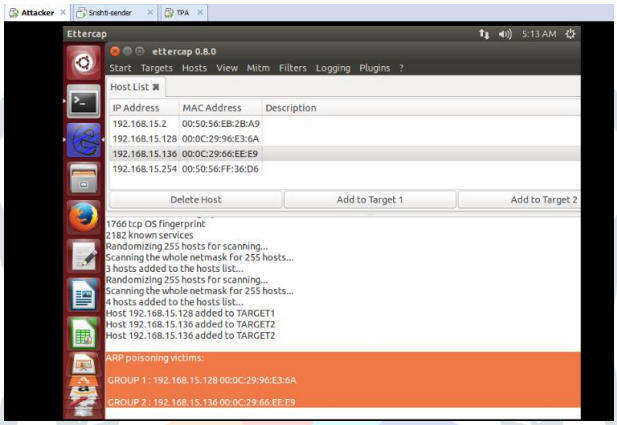

Figure 5 Man in middle Attack in Attacker machine

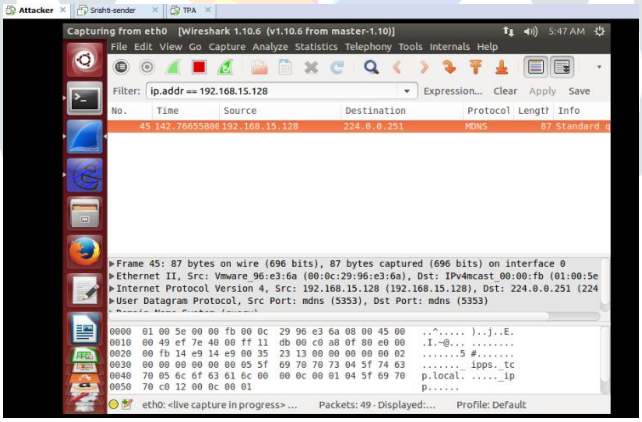

Figure 6 Capturing data from eth0

TPA detect ARP duplication and other information as shown in Figure 7 using Wireshark. By using Firewall- IPTables rules TPA block attacker as shown in Figure 8.

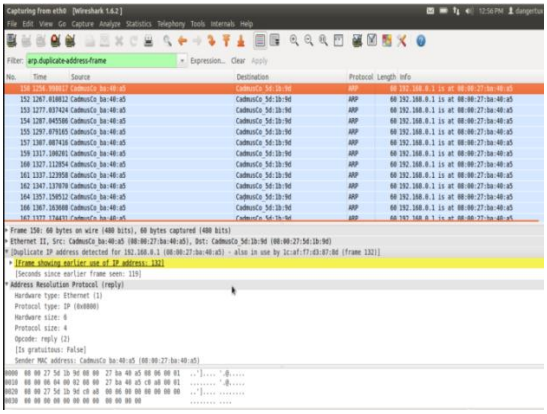

Figure 7 detect ARP duplication and other information

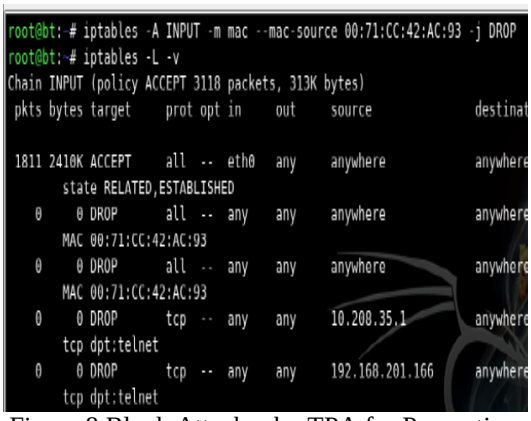

Figure 8 Block Attacker by TPA for Prevention

Sender send Image that is monitor by TPA. It is first compare by TPA. If it is mathch then forwarded to the Receiver as shown in Figure 9 and Figure 10.

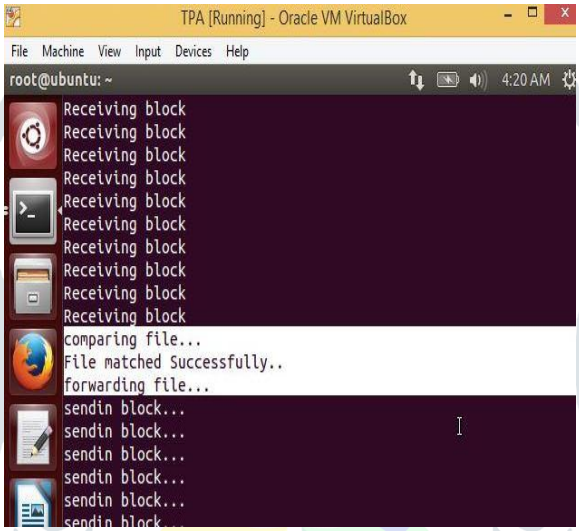

Figure 9 Compare file by TPA

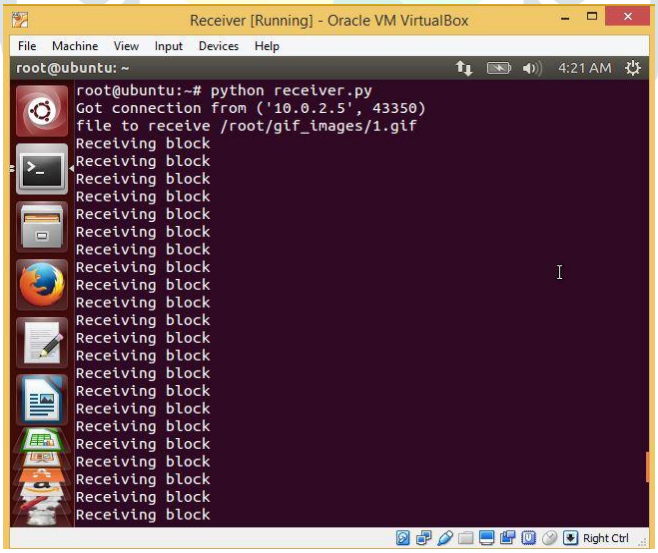

Figure 10 Receiver receive animated GIF Image

VII. RESULT ANALYSIS AND COMPARISON OF METHODS

As I explain in Introduction in Table 1 Quality of Steganographed Image is Better in LSB than DCT, DWT. The larger the PSNR value decreases the possibility of visual attacks by human eye. Higher PSNR value indicates better quality of image.Peak signal-to-noise ratio is most easily de_ned via the mean squared error (MSE).PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The PSNR (in dB).The MSE is the cumulative squared error between the compressed and the original image, whereas PSNR is a measure of the peak error. The mathematical formula for the two are:

$$MSE = \frac{1}{MN} \sum_{y=1}^{M} 0 \sum_{x=1}^{N} [I(x,y) - I(x,y)]2^2 \qquad (1)$$

$$PSNR = 20 * \log 10\ (255 / sqrt(MSE)) \qquad (2)$$

where I(x,y) is the original image, I'(x,y) is the approximated version (which is actually the decompressed image) and M,N are the dimensions of the images. A lower value for MSE means lesser error, and as seen from the inverse relation between the MSE and PSNR, this translates to a high value of PSNR. Logically, a higher value of PSNR is good because it means that the ratio of Signal to Noise is higher. Here, the 'signal' is the original image, and the 'noise' is the error in reconstruction. So, if you find a compression scheme having a lower MSE (and a high PSNR), you can recognise that it is a better one. Table shows PSNR values of Different types of images. LSB has high PSNR value that DCT and DWT. So, Quality of Image is Better in LSB than DCT and DWT. Figure 8.1 shows Comparison graph of that. we are focusing in quality of steganographed image that's why we use LSB Embedding.

Figure 11 PSNR value in db of Different Images in LSB DCT DWT Method

VIII. CONCLUSION

Our system is used for detect ooze that happened by external entity on GIF image. Till now only bmp, jpeg and png images are used in data leakage as per on survey. In our system detection of ooze is done by trusted third party auditor. Firewall system is used for preventing system from attacker by TPA. In our proposed method we use LSB embedding method to hide data. After embedding, changes in color image or grayscale are not visually observable that is advantages of LSB Embedding.

REFERENCES

[1] Sayali Patil Tanzila Patel A.A. Deshmukh Aishwarya Kulkarni, Priyanka Jagtap. A survey of data leakage detection algorithms in server. In Technical Journal of the International of Engineers(India) Pune Local Center under the aegis of ICC, Vol.39, pages 164-167, 2015.

[2] Hector Garic Monila Panagiotis Papadimitriou. Data leakage detection. In Transactions on knowledge and data engineering, Vol 23, No. 1, pages 433-435. IEEE,2011.

[3] Guraraj Maddodi Saul Gill Brian Lee Abir Award, Sara Kadry. Data leakage detection using system call provenance. In International Conference on Intelligent Networking and Collaborative systems, pages 486-491. IEEE, 2016.

[4] Ting Gao Ryan K L Ko, Alan Y S Tan. A mantrap-inspired, user-centric data leakage prevention (dlp) approach. In 6th International Conference on Cloud Computing Technology and Science, pages 1033-1039. IEEE, 2014.

[5] Jun Ma Songzhu Mei Jiangchun Ren Jiangjiang Wu, Jie Zhou. An active data leakage prevention model for insider threat. In International Symposium on Intelligence Information Processing and Trusted Computing, pages 39-42. IEEE, 2011.

[6] S.S. Dhotre P.P. Dandavate. Data leakage detection using image and audio _les. In International Journal of Computer Applications Vol 115-No. 8, pages 1-4, 2015.

[7] Bhagyashri P. Yeola Rakesh Badodekar Sanchit S. Mhatre, Vaibhav V. Kakhandai. Data leakage detection using lsb. In International Journal of Advanced Research in Computer and Communication Engineering Vol. 4,Issue 3,, pages 433-435, 2015.

[8] Himanshu Mishra Hitendra Garg Neeraj Kumar, Vijay Katta. Detection of data leakage in cloud computing environment. In Sixth International Conference on Computational Intelligence and Communication Networks, pages 803-807. IEEE,
2014. J. Venkata Rao Anusha Koneru, G. Siva Nageswara Rao. Data leakage detection using encrypted fake objects. In International Journal of P2P Network Trends and Technology- Vol 3 Issue 2, pages 104-110, 2013.

[9] Kapil Garg Vahid Inamdar Ankit Agarwal, Mayur Gaikwad. Robust data leakage and email _ltering system. In International Conference on Computing, Electronics and Electrical Technologies[ICCEET], pages 1032-1035. IEEE, 2012.

[10] R. S. Shaji T. Brindha. An analysis of data leakage and prevention techniques in cloud environment. In International Conference on Control, Instrumentation, Communication and Computational Technologies(ICCICCT), pages 350-355. IEEE,2015.

[11] Saroj Kumar Mamta Jain. A review on data leakage prevention using image steganography. In International Journal of Computer Science Engineering (IJCSE),pages 56-59, 2016.

[12] Chen Ting Li Hua Zhang Xiaosang, Liu Fei. Research and application of the transparent data encryption in intranet data leakage prevention. In International Conference on Computational Intelligence and security, pages 376-379. IEEE, 2009.

[13] Richard Overill Veroniki Stamati-Koromina, Christos Ilioudis. Insider threats in corporate environments: A case study for data leakage prevention. pages 271-274.ACM, 2012.

[14] B. Padmaja Rani Subhashini Peneti. Data leakage prevention system with time stamp. In International Conference on Information Communication and Embedded System (ICICES), pages 978-981. IEEE, 2016.

[15] K. Deepthi Narendra Babu Pamula, M. Siva Naga Prasad. Preventing data leakage in distributive strategies by steganography technique. In International Journal of Computer Science and Information Technologies, Vol 4,pages 220-223, 2013