International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 6 Issue 4, April-2017, Impact Factor: 1.544

Software Security Analysis with Cryptography using MAC Address

Shashi Bala

M. Tech Student, Dept. of CSE, R N College of Engg., Rohtak, Haryana

ABSTRACT

Most important issues to software developers are Software piracy, software licensing and license control. Small software developers did not have access to a system available to control a number of installations of licensed software products. A company could obtain a single license and use in among the network, or there could be a breach of security allowing multiple users to use fully licensed software on many different computers. Software Privacy is built to protect the privacy of its users. The software typically works in conjunction with Internet usage to control or limit the amount of information made available to third parties. The software can apply encryption or filtering of various kinds. Most retail programs are licensed for use at just one computer or for use by only one user at any time. By buying the software, you become a licensed user rather than an owner. You are allowed to make copies of the program for backup purposes, but it is against the law to give copies to friends and colleagues.

INTRODUCTION

An online license management system helps reduce both forms of piracy by ensuring that each copy of the software product being installed is legal and has been installed on a PC in compliance with its license terms. Installations beyond those allowed in the license agreement will fail to activate, thus preventing both casual and intended piracy. There are certain ways to prevent or restrict those illegal activities. One way is tying software installation to hardware. Hardware tying, however, has a huge drawback to software publishers: a user has to pass a Hardware ID to the software manufacturer at the time of ordering, which might his willingness to purchase that product at all, playing its role in the decision of getting this or competitor's product. Additionally, a user will have to manually obtain a Hardware ID and pass it to the ordering system, which is usually implemented as a SSL-encrypted Web order form. Another way is Product Activation. Product activation is a license validation procedure required by some proprietary computer software programs. Product activation prevents unlimited free use of copied or replicated software. Inactivated software refuses to fully function until it determines whether it is authorized to fully function. Activation allows the software to stop blocking its use. Activation can last "forever", or it can have a time limit, requiring a renewal or re-activation for continued use.

Software that has been installed but not activated does not perform its full functions, and/or imposes limits on file size or session time. Some software allows full functionality for a limited "trial" time before requiring activation. Inactivated software typically reminds the user to activate, at program startup or at intervals, and when the imposed size or time limits are reached. (Some inactivated software has taken disruptive actions such as crashing or vandalism, but this is rare.)

Some 'inactivated' products act as a time-limited trial until a product key—a number encoded as a sequence of alphanumeric characters—is purchased and used to activate the software. Some products allow licenses to be transferred from one machine to other using online tools, without having to call technical support to deactivate the copy on the old machine before reactivating it on the new machine.

Software verifies activation every time it starts up, and sometimes while it is running. Some software even "phones home", checking a central database (across the Internet or other means) to check whether the specific activation has been revoked. Some software might stop working or reduce functionality if it cannot connect to the central database.

Due to piracy and other forms of unauthorized use, users cannot always be sure that they have a genuine copy of software. The goal of product activation is to reduce a form of piracy known as casual copying. Casual copying is the sharing and installation of software that is not in compliance with the software's end user license agreement and is estimated to contribute to half of all pirated installations. Product Activation helps ensure that each copy is installed in

compliance with the end-user license and is not installed on more than the limited number (usually one) of computers allowed by the product license.

Software

Computer software, or simply software, is that part of a computer system that consists of data or computer instructions, in contrast to the physical hardware from which the system is built. In computer science and software engineering, computer software is all information processed by computer systems, programs and data. Computer software includes computer programs, libraries and related non-executable data, such as online documentation or digital media. Computer hardware and software require each other and neither can be realistically used on its own.

At the lowest level, executable code consists of machine language instructions specific to an individual processor—typically a central processing unit (CPU). A machine language consists of groups of binary values signifying processor instructions that change the state of the computer from its preceding state. For example, an instruction may change the value stored in a particularstorage location in the computer—an effect that is not directly observable to the user. An instruction may also (indirectly) cause something to appear on a display of the computer system—a state change which should be visible to the user. The processor carries out the instructions in the order they are provided, unless it is instructed to "jump" to a different instruction, or is interrupted (by now multi-core processors are dominant, where each core can run instructions in order; then, however, each application software runs only on one core by default, but some software has been made to run on many).

The majority of software is written in high-level programming languages that are easier and more efficient for programmers, meaning closer to a natural language. High-level languages are translated into machine language using a compiler or an interpreter or a combination of the two. Software may also be written in a low-level assembly language, essentially, a vaguely mnemonic representation of a machine language using a natural language alphabet, which is translated into machine language using an assembler.

LITERATURE REVIEW

N. K. Kamila, Haripriya Rout said that Information protection is now a crucial problem and good solution to this problem is cryptography and steganography. The content of message is kept secret in cryptography, where as in Steganography; a message is embedded in a cover image. In our proposed work a system is developed in which LSB Steganography and Cryptography using chaotic neural network is combined together to provide high security to the message during communication in an unsecure channel. In LSB Steganography taking advantage of the way the human eye perceives images, the technique involves of replacing the N least significant bits of each pixel of a container image with the data of a hidden message. Cryptography based on chaotic neural network is used because of its noise like behaviour which is quite significant for cryptanalyst to know about the hidden information as it is hard to predict. Thus the information is being kept secret. In this work we have considered the advantages of both the concepts and developed a model in which initially a message is embedded in a gray scale image using LSB steganography and then the stegoimage is encrypted using chaotic neural network to provide high security to the message. The whole process is implemented using MATLAB. The simulation results show the robustness of the technique.

Nentawe Y. Goshwe One of the principal challenges of resource sharing on data communication network is its security. This is premised on the fact that once there is connectivity between computers sharing some resources, the issue of data security becomes critical. This paper presents a design of data encryption and decryption in a network environment using RSA algorithm with a specific message block size. The algorithm allows a message sender to generate a public keys to encrypt the message and the receiver is sent a generated private key using a secured database. An incorrect private key will still decrypt the encrypted message but to a form different from the original message

Vishwa gupta, Gajendra Singh to write this paper I have Study about information security using cryptography technique. After the detailed study of Network security using cryptography, I am presenting my proposed work. This paper is dividing in four sections. In section-I, I am presenting just basic introduction about Information Security using cryptography, in section-II, I am presenting detailed description of Information security using cryptography and various algorithms, in section-III, I am presenting my proposed algorithm, and in section IV I am Presenting summary and references where I have completed my research. The proposed algorithm has the batter speed compared with the comparing encryption algorithm. Nevertheless, the proposed algorithm improves encryption security by inserting the symmetric layer. The proposed algorithm will be useful to the applications which require the same procedure of encryption and decryption.

Dr. Mohammed Abbas Fadhil Al-Husainy committed that in computer networking, the Media Access Control (MAC) address is a unique value associated with a network adapter. MAC addresses are also known as hardware addresses or physical addresses. TCP/IP and other mainstream networking architectures generally adopt the OSI model.

MAC addresses function at the data link layer (layer 2 in the OSI model). They allow computers to uniquely identify themselves on a network at this relatively low level. In this paper, suggested data encryption technique is presented by using the MAC address as a key that is used to authenticate the receiver device like PC, mobile phone, laptop or any other devices that is connected to the network. This technique was tested on some data, visual and numerical measurements were used to check the strength and performance of the technique. The experiments showed that the suggested technique can be used easily to encrypt data that is transmitted through networks.

Ram D. Gopa G. Lawrence Sanders said that in an attempt to protect their intellectual property and compete effectively in an increasingly dynamic marketplace, software publishers have employed a number of preventive and deterrent controls to counter software piracy. Conventional wisdom suggests that reducing piracy will force consumers to acquire software legitimately, thus increasing firm profits. We develop an analytical model to test the implications of antipiracy measures on publisher profits. Our results suggest that preventive controls decrease profits and deterrent controls can potentially increase profits. Empirical results are also presented that support the proposition on the impact of deterrent controls on the extent of software piracy derived from the analytical model.

Laurie E. MacDonald et al. argued that although software piracy has serious implications for the software industry and the economy, the topic receives very little detailed coverage in MIS textbooks. Software piracy has a significant impact on the software industry and on the economy as a whole. Lost sales due to software piracy amount to over $11 billion annually and lost taxes approach $1 billion annually. Current technology makes it a simple task for even a novice computer user to copy software and therefore, unauthorized software is not uncommon. The researchers conducted an evaluation of MIS texts and found that software piracy receives very little coverage in the texts. The research suggests that MIS faculty need to provide material to supplement the textbook coverage in order to provide adequate coverage of this serious issue.

Susan Athey et al. evaluated the nature, relative incidence and drivers of software piracy. In contrast to prior studies, they analyze data that allows us to measure piracy for a specific product – Windows 7 – which was associated with a significant level of private sector investment. Using anonymized telemetry data, we are able to characterize the ways in which piracy occurs, the relative incidence of piracy across different economic and institutional environments, and the impact of enforcement efforts on choices to install pirated versus paid software. They find that: (a) the vast majority of "retail piracy" can be attributed to a small number of widely distributed "hacks" that are available through the Internet, (b) the incidence of piracy varies significantly with the microeconomic and institutional environment, and (c) software piracy primarily focuses on the most "advanced" version of Windows (Windows Ultimate). After controlling for a small number of measures of institutional quality and broadband infrastructure, one important candidate driver of piracy – GDP per capita – has no significant impact on the observed piracy rate, while the innovation orientation of an economy is associated with a lower rate of piracy. Finally, they are able to evaluate how piracy changes in response to country-specific anti-piracy enforcement efforts against specific peer-to-peer websites; overall, they find no systematic evidence that such enforcement efforts have had an impact on the incidence of software piracy.

PROBLEM FORMULATIONS

Software piracy is the unauthorized copying, reproduction, use, or manufacture of software products. On average, for every authorized copy of computer software in use, at least one unauthorized or "pirated" copy is made. In some countries or regions, up to 99 unauthorized copies are made for every authorized copy in use. Software piracy harms everyone in the software community including you, the end user. Piracy results in higher prices for duly licensed users, reduced levels of support, and delays in the funding and development of new products, causing the overall selection and quality of software to suffer.

Piracy harms all software publishers, regardless of their size. Software publishers spend years developing software for the public to use. A portion of every dollar spent in purchasing original software is funneled back into research and development so that better, more advanced software products can be produced. When you purchase pirated software, your money goes directly into the pockets of software pirates instead.

Software piracy also harms the local and national economies. Fewer legitimate software sales result in lost tax revenue and decreased employment. Software piracy greatly hinders the development of local software communities. If software publishers cannot sell their products in the legitimate market, they have no incentive to continue developing programs. Many software publishers won't enter markets where the piracy rates are too high, because they will not be able to recover their development costs.

Financial Impact Worsening

The software piracy rate can be estimated by comparing the number of personal computers sold with the number of software packages sold. Based on the assumption that for each new PC, a standard set of software would also be sold, the software piracy rate is calculated as the percentage shortfall in software sales. The financial loss is then the cost of

these missing software sales. Using this method, the Software and Information Industry Association (SIIA) and the Business Software Alliance (BSA) estimate that the software industry lost $12.2 billion in revenue in 1999 due to the pirating of business software. This is an increase from the 1998 figure of $11 billion and brings the estimated losses since the surveys began in 1994 to a total of $71.4 billion.

The world's highest software piracy rates are in Eastern Europe and the Middle East, with rates of more than 60 percent, suggesting that six out of every ten software packages used are pirated. Fourteen countries are estimated to have a software piracy rate above 80 percent, with Vietnam (98 percent), China (91 percent), Russia (89 percent), and Oman (89 percent) at the top of the list.

Because of the size of their respective software markets, however, the greatest financial losses occur in the United States, Japan, the United Kingdom, France, China, and Germany. These six countries accounted for $6.7 billion, or more than half of worldwide lost sales in 1999. Although the United States had the lowest piracy rate in the world at 25 percent for 1999, the United States alone accounts for more than $3 billion in lost sales.

The problems in the existing system as

- For online registration of application software internet is required, which may be not available in some remote areas.
- By making the image of CD/DVD software is copied, which is lack of piracy control.
- It's very difficult to visit the client site for license registration of software on client system by software owner company
- Software may be cracked when company provide the CD key with software CD.

The most widely used method is the license key; code that is built into an application to require a valid key to unlock the software. This key can be distributed via packaging or some other online mechanism. But this technique may be cracked for the software piracy. To solve this problem we have implemented the software protection by licensed key using MAC Address and the concept of cryptography

Because of greater demand in digital signal transmission in recent time, the problem of illegal data access from unauthorized persons becomes need intelligent and quick solution. Accordingly, the data security has become a critical and imperative issue in multimedia data transmission applications. In order to protect valuable information from undesirable users or against illegal reproduction and modifications, various types of cryptographic/encryption schemes are needed. Cryptography offers efficient solutions to protect sensitive information in a large number of applications including personal data security, medical records, network security, internet security, diplomatic and military communications security, etc. through the processes of encryption/decryption. Cryptography contains two basic processes: one process is when recognizable data, called plain data, is transformed into an unrecognizable form, called cipher data. To transform data in this way is called to encipher the data or encryption. The second process is when the cipher data is transformed back to the original plain data, this is called to decipher, or decrypting the data. To be able to determine if a user is allowed to access information a key is often used. Once a key has been used to encipher information, only someone who knows the correct key can decipher the encrypted data. The key is the foundation of most data encryptions algorithms today. A good encryption algorithm should still be secure even if the algorithm is known.

RESULTS & DISCUSSION

Cryptography through MAC address provides more security to the vendor product. It is more users friendly. It has version number, so we can make further implementation to it. It is platform independent. It gives fast performance. Establishes relation between customer and vendor. Most important any user could not be crack this license file and cannot use illegally, because this license file is generated by encryption process and which is in binary format. Software License Keys are used in various copy protection schemes. The basic idea is that only users that have acquired the appropriate license will be issued a license key enabling them to install or use the software.

The key itself can be a string of characters entered into the installer or the software itself which by some method of computational comparison verifies the entered key and subsequently continues the installation process or the execution of the software. The key can also be a hardware dongle that physically connects with the computer making the key less vulnerable to copying. Generally speaking, circumventing copy protection schemes based on either software license keys or hardware dongles through reverse engineering of the verification code is not complicated unless rigorous code protection mechanisms are put in place to obfuscate the copy protection itself. Bear in mind that all protection systems can (and will be given enough time and resources) broken.

In the figure 1 System Date is 24th February 2015. When we enter first time Username and Password the mac_address table is blank as shown in the figure 2. This Print screen shows mac_address table is blank when we install the software and enter first time username and password.

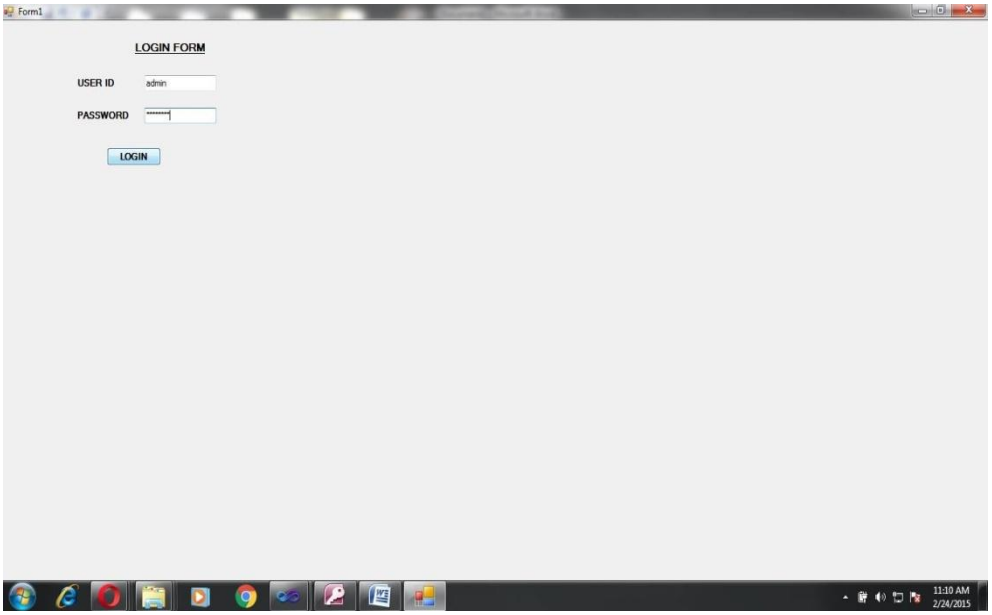

Figure 1: Print Screen of Login Form

When we click on submit button of login form, then the main admin form opens. Figure 2 shows the UI of the form named form1 in my project.

Fig 4.2: Print Screen of the UI of the form named form1

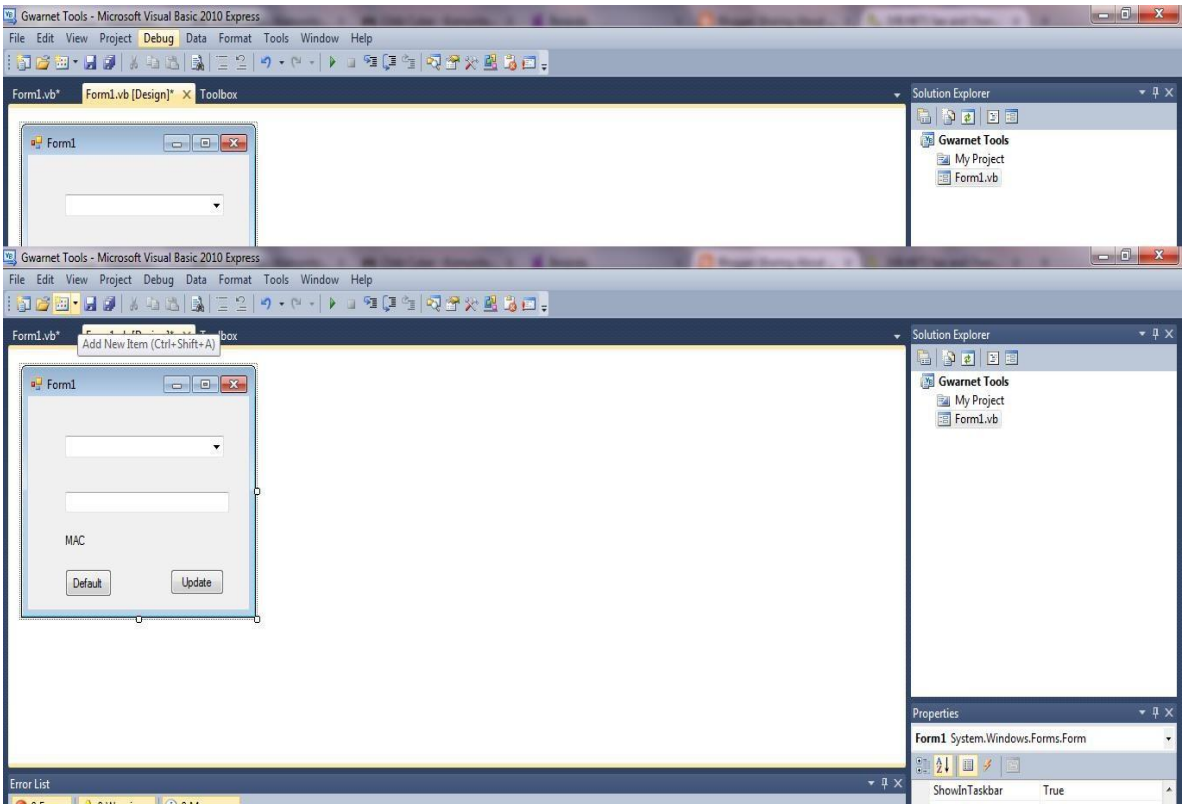

Fig 2: Print Screen of the UI of the form named form1

A. Key space analysis in any effective encryption system, the key space should be large enough to make brute-force attack infeasible. The secret key space (MAC address) in the suggested technique is (6bytes = 48bits), this means that the encryption system has relatively enough number of bits in the secret key. In this work, we note that the bits in the key are restricted by the MAC address and they cannot be increased or decreased.

B. Key sensitivity to evaluate the key sensitivity feature of the proposed technique, a one bit change is made the secret key (MAC address) and then used it to decrypt the encrypted image. The decrypted image with the wrong key is completely different when it is compared with the decrypted image by using the correct key as shown in Fig. 3. It is the conclusion that the proposed encryption technique is highly sensitive to the key, even an almost perfect guess of the key does not reveal any information about the plain image/data.

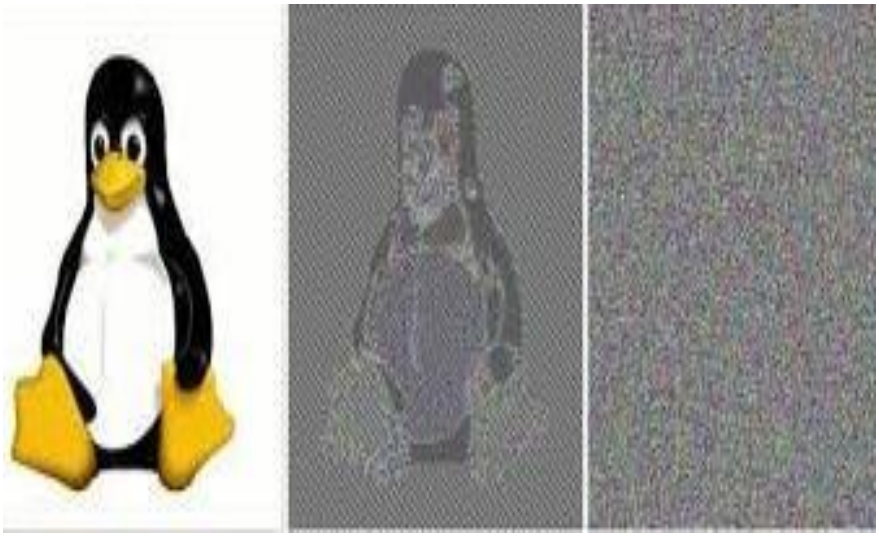

Figure 3: (a) Source image (b) Encrypted image (c) Decrypted image with wrong key

C. Statistical analysis Statistical attack is a commonly used method in cryptanalysis and hence an effective encryption system should be robust against any statistical attack. Calculating the histogram and the correlation between the neighbors pixels in the source and in the encrypted image are the statistical analysis to prove the strong of the proposed encryption system against any statistical attack.

CONCLUSIONS

With the rapid growth of information technology, there has been an increasing trend to digitalize tools and information and move away from the traditional forms of doing business. This rapid advancement has been seen for the most part as positive. Unfortunately it has lead to a number of unforeseen problems. Copyright laws that had originally been suited for physical texts and tools could no longer be applied to digital works. The entire notion of property as something necessarily physical has transformed into something more abstract, giving rise to the concept of intellectual property. Intellectual property is defined as anything created using one's intellect. This includes computer software, books, art, schematics, music, and other creative works. With the concept of intellectual property came new legislation to protect these works. Unfortunately, this legislation, though it prohibits software piracy, has been insufficient to prevent widespread piracy in most of the world.

The protection scheme presented in this thesis overcomes the fundamental flaws common to almost all existing technical means for software piracy prevention. The protection mechanism migrates from static nature of defense to a dynamic nature. The marginal cost of using the software decreases. Of the existing technique, software aging is of dynamic nature but the number of forms of software privacy against which it provides protection is too late. The copy rights to run the software on client/customer machine are only available to the software developer company.

The only drawback of the scheme occurs when the user has changed its LAN Card/ Motherboard, the Mac address is also changed and the user has to send the request to software Developer Company to send the License key again. In future we can improve this drawback. Also, a technique for data encryption has been presented which employ the MAC address of the receiver device to use it as a key for encryption. This technique made a good immunity for the data that is transmitted through networks. The visual and analytical tests showed that the suggested technique is useful to use in the field of image/data encryption effectively in networks.

REFERENCES

[1]. Daniel, L.C, 2008. "Literature Review of cryptography and its role in Network security", Principles and Practice , Capella University, pp. 1-20.
[2]. Bin G. and Qian, 2009. "A new image encryption scheme based on DES algorithm and Chua's circuit", International Workshop on Imaging Systems and Techniques, South university of Technology, Shenzhen, pp. 168-172.
[3]. Bin, L., Lichen, L., Jan Z., 2010. "Image encryption algorithm based on chaotic map, and S-DES", Advanced Computer Control (ICACC), 2nd International Conference, Information & Computer Engineering College, Northeast University, Harbin, China. pp. 41-44.
[4]. Alani M.M., 2010. "DES96-Improved DES Security", 7th International Multi conference on Systems, Signals & Devices, Gulf Univ., Gulf, Bahrain, pp. 1-4.
[5]. Alaa A.H, Mohammad A., Soukaena H.H, 2011. "A proposed Modified Data Encryption Standard algorithm by Using Fusing Data Technique", World of Computer Science and Information Technology Journal, Vol. 1, No. 3, pp. 88-91.
[6]. Said F.Z, Y.A.Nada, A.A. Abdo, 2011. "How Good Is The DES Algorithm In Image Ciphering", Int. J. Advanced Net-working and Applications, Vol.02, pp. 796-803.
[7]. Sumedha Kaushik and Ankur Singhal(2012), "Network Security Using Cryptographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12.
[8]. Jashanpreet Pal Kaur and Rajbhupinder Kaur(2014), "Security Issues and Use of Cryptography in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7.
[9]. Laurie E. MacDonald and Kenneth T. Fougere, "Software Piracy: A Study of the Extent of Coverage in Introductory MIS Textbooks", Journal of Information Systems Education, Vol. 13(4).
[10]. Susan Athey and Scott Stern(2014), "The Nature and Incidence of Software Piracy: Evidence from Windows".
[11]. Thai Duong and Juliano Rizzo(2011), "Cryptography in theWeb: The Case of Cryptographic Design Flaws in ASP.NET", IEEE Symposium on Security and Privacy.
[12]. Walt Scacchi and Thomas Alspaugh, "Addressing Challenges in the Acquisition of Secure Software Systems with Open Architectures".