SOFTWARE ACTIVATION AND PIRACY PROTECTION USING STEGANOGRAPHY

ALAN ALEXANDER

MCA

INFORMATION SECURITY MANAGEMENT SERVICES

Jain University Bangalore, India

Abstract: Software Activation And Piracy Protection Using Steganography application is to develop a web portal where various software's are available for download. The downloaded software is able to run only after the payments are made properly which is titled as software activation. Also downloaded software should run on the particular computer only. If the user copies the software to another computer then it should not run which is titled as Piracy Protection. The system uses Steganography Technique to achieve this. The application contains two sessions with respect to Admin and the user. After the successful authentication process, the user would be given access to view the existing application and thus downloading the software with the concept of Steganography at behind the scene. The admin will be responsible for the complete maintenance of the entire session that is needed for a user to be authenticated.

I. INTRODUCTION

Software piracy is the act of making unauthorized copies of computer software. Software piracy is a major concern for software providers, even though there is currently many defence mechanisms that have been used to prevent it. This paper identifies the weaknesses of existing approaches, resulting mainly because most of them are having a static nature of defence and the impossibility to prevent the duplication of digital data and commercial software. A new solution is proposed which can solve the problem of software piracy to an extent using steganography.

2.Scope of the Product

Developing a web portal where various software are available to download, the downloaded software is able to run only when the payments are made properly that we call it as software activation. Also downloaded software should run on the particular computer only, if the user copy the software to another computer then it should not run that is Piracy Protection. This system uses Steganography Technique to achieve this. While online payment is taking place, this system will ask for the C: volume Serial number and Physical IP Address of the computer where the user want to run the software. Once payment is done this system will generate "Activation Code" using the C: volume serial number and Physical IP Address and the Activation Code is inserted into a Image using Steganography Technique. This Image is send to the user and informs the user to keep this image to run the downloaded application. The project first gets the C: Volume Serial Number and Physical IP Address from the user and generate the activation code and that data is attached to the image in such a way that it does not destroys the views of the image. The colour, appearance and other attributes of the image is not damaged or damage may be very negligible. Then the image file can be transferred to the user. The algorithm for detaching the activation code from the image is written in the application.

3.Existing System

Piracy is a big problem in the software industry. Now a Day, a user is able to purchase the software through websites. While the user is purchasing the software through websites, he has to under the payment procedure after which will be the software is downloaded.
 In the existing system, while the payment procedure is going through, the system to which the software is downloaded is not authenticated; which would rather result in running of the same application in multiple systems though the buyer would be one.
The above problem is a gateway for the user to run a free copy of the software in the personal system without any payments which would result in the big loss for a software company. To avoid the existing problem with regard to the piracy issues, the new system has been proposed which could better act as a boon incentively.

4. Proposed System

Developing a web portal where various software are available to download, the downloaded software is able to run only when the payments are made properly that we call it as software activation. Also downloaded software should run on the particular computer only, if the user copy the software to another computer then it should not run that is Piracy Protection. This system uses Steganography Technique to achieve this.
 While online payment is taking place, this system will ask for the C: volume Serial number and Physical IP Address of the computer where the user want to run the software. Once payment is done this system will generate "Activation Code" using the C: volume

serial number and Physical IP Address and the Activation Code is inserted into a Image using Steganography Technique. This Image is send to the user and informs the user to keep this image to run the downloaded application.

5.Steganography in the Project

The project first gets the **C: Volume Serial Number** and **Physical IP Address** from the user and generate the activation code and that data is attached to the image in such a way that it does not destroys the views of the image. The color, appearance and other attributes of the image is not damaged or damage may be very negligible. Then the image file can be transferred to the user. The algorithm for detaching the activation code from the image is written in the application.

6. Encryption And Decryption

This project uses XOR Operation for Encryption And Decryption.

7. Project Module Description
Admin Session
- Login Module
- User Details (Delete & Update)
- Image Maintenance
- Change Password

User Session
- User Registration
- Login Module
- View the Existing Application
- Downloading the Application
- Payment Gate Way
- Generating the Activation code based.
- Hiding the Activation code into Image using Steganography.
- Change Password

8. Window Application Functionalities
While Running the Application
- Extracting Activation Code from Image
- Extracting C: Volume Serial No and Physical IP Address from the current system.
 Comparing the activation code with the extracted data from current System and run the application.

9. Language Description

FRONT END TECHNOLOGY:-

JAVA TECHNOLOGY:-

Initially the language was called as "oak" but it was renamed as "Java" in 1995. The primary motivation of this language was the need for a platform-independent (i.e., architecture neutral) language that could be used to create software to be embedded in various consumer electronic devices.

Java is a general-purpose computer-programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere" (WORA), meaning that compiled Java code can run on all platforms that support Java without the need for recompilation. Java applications are typically compiled to bytecode that can run on any Java virtual machine (JVM) regardless of computer architecture. As of 2016, Java is one of the most popular programming languages in use, particularly for client-server web applications, with a reported 9 million developers. Java was originally developed by James Gosling at Sun Microsystems (which has since been acquired by Oracle Corporation) and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++, but it has fewer low-level facilities than either of them.

• 　　Java is a programmer's language.

- Java is cohesive and consistent.

- Except for those constraints imposed by the Internet environment, Java gives the programmer, full control.

- Finally, Java is to Internet programming where C was to system programming.

BACK END TECHNOLOGY:-

MYSQL SERVER:-

Microsoft SQL Server is a Structured Query Language (SQL) based, client/server relational database. Each of these terms describes a fundamental part of the architecture of SQL Server.

 DATABASE:-

A database is similar to a data file in that it is a storage place for data. Like a data file, a database does not present information directly to a user; the user runs an application that accesses data from the database and presents it to the user in an understandable format. A database typically has two components: the files holding the physical database and the database management system (DBMS) software that applications use to access data. The DBMS is responsible for enforcing the database structure, including: Maintaining the relationships between data in the database. Ensuring that data is stored correctly and that the rules defining data relationships are not violated. Recovering all data to a point of known consistency in case of system failures.

10. Advantages

- This System can be used by any software company.

- And also can be used by any other organization to protect product copyright.

- No third party can install the software.

- Can only be installed using activation image.
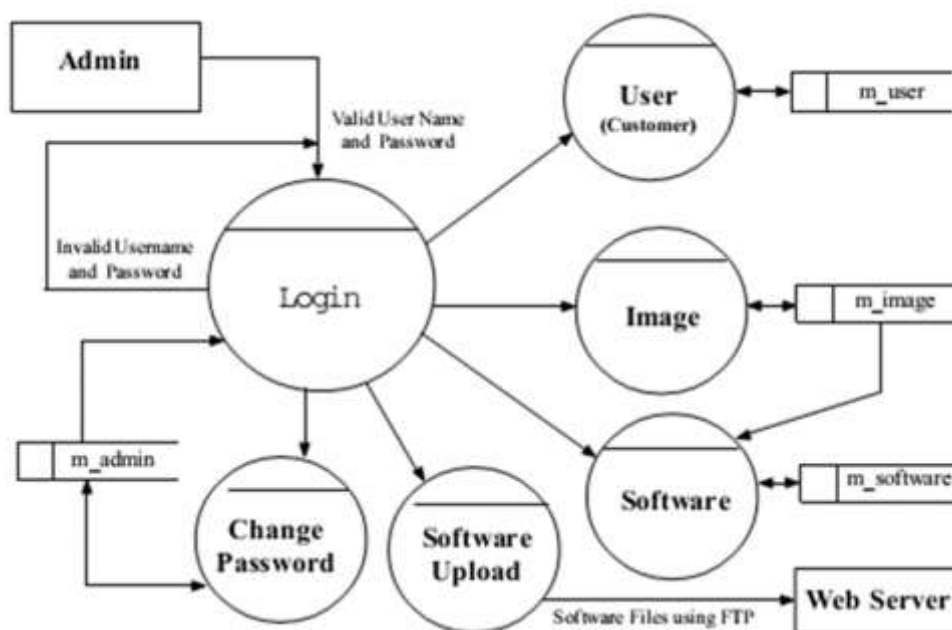
- Achieved through steganography.

11. Limitations

There are few limitations but can be enhanced in future. Since it uses MAC address, it cannot be installed on multiple systems.
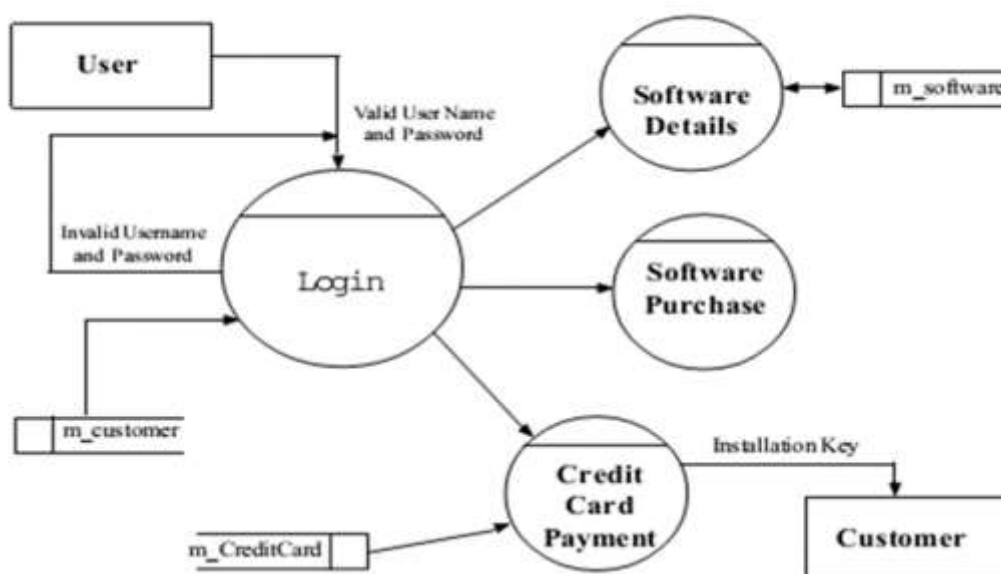
12. Context Diagram
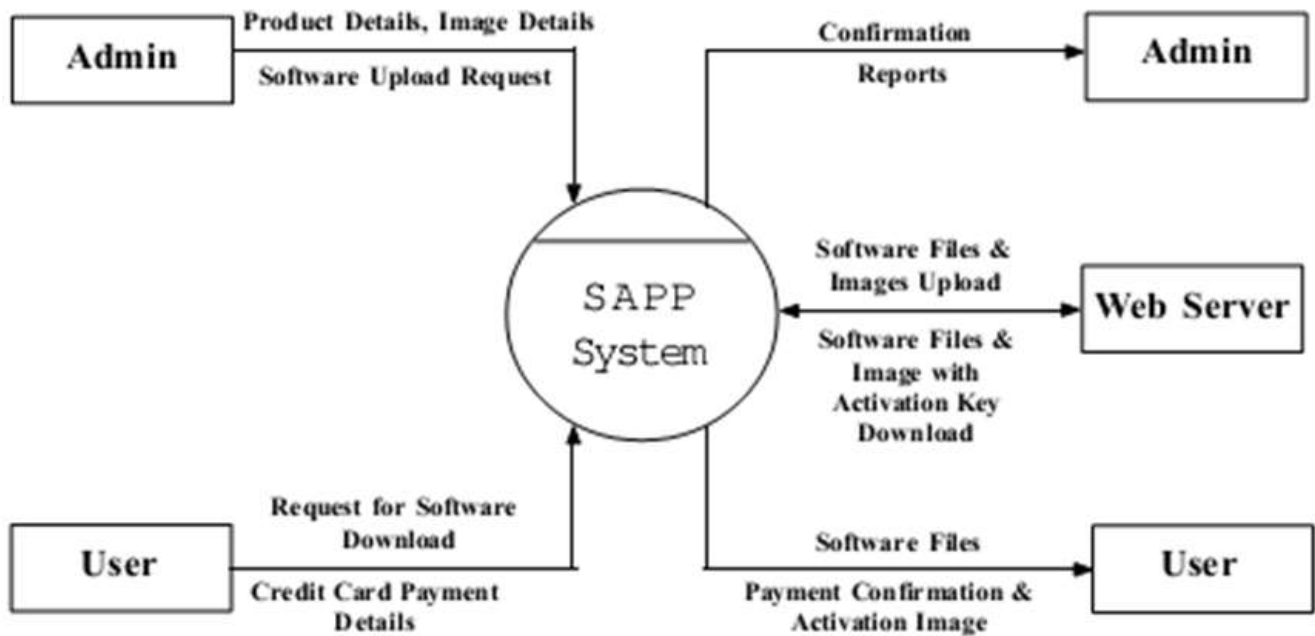
13. Dataflow Diagrams

Admin:

User:

14. Conclusion

This project we used steganography technique for protection of software piracy to prevent unauthorized access,.This system provides more security to the software. Software piracy is a serious issue that impacts the bottom line for software developers. By implementing steganographyfor software protection, software developers can gain the benefits of protection from piracy as well as obtain the ability to implement more license models. A security implementation plan that balances the time and resources with the desired outcome is possible given the wide range of security options. Developers can use steganography method to prevent software piracy.

15. ACKNOWLEDGMENT

16. REFERENCES

- Diffie, W., and Hellman, M.E., New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, no. 6, November 1976, pp.
- Garret, Paul. Making, Breaking Codes: An Introduction to Cryptology. Upper Saddle River, NJ: Prentice-Hall, 2001
- Hoffstein, Jeffery, Pipher, Jill and Silverman, Joseph H. NTRU: A Public Key Crypto http://grouper.ieee.org/groups/1363/lattPK/submissions.html#NTRU1
- Kurose, James F., Ross, Keith W., Computer Networking: A top Down Approach Featuring the Internet. 2nd edition. Addison Wesley 2002.
- J. Algesheimer, C. Cachin, J. Camenisch, G. Karjoth, "Cryptographic Security for Software", pp. 2–11 in Proc. 2011 IEEE Symposium on Security and Privacy (May 2011).
- "The History of software piracy [infographic],"[online] 2011, http://churchm/software-piracyhistory/(Accessed: 18 October 2013).
- "Digital Millennium Copyright Act,"[online] 2011, http://whatis.techtarget.com/definition/Digit al-Millenium-Copyright-Act-DMCA/ (Accessed:18 October 2013).
- "Digital Millennium Copyright Act,"[online] 1998, http://www.copyright.gov/legislation/hr2281 .pdf(Accessed:18October 2013).
- http://www.seopher.com/images/softwarepiracy-2007.jpg [
- "Software Piracy: Study Claims 57 Percent of the World Pirates Software,"[online]2012,http://www.huffingt onpost.com/2012/06/01/software-piracystudy-bsa_n_1563006.html (Accessed: 18 October 2013).
- en.wikipedia.org.
- www.codenotes.com
- www.dotnetspider.com

BIOGRAPHY

Prof. Subarna Panda
M.Tech(CSE)
Working as Professor Jain University Jayanagar, Bangalore
Department Computer Science Information Techology

Alan Alexander
Master Computer Application (Information Security and Management Services)
Intern at Niyo Solutions