Product Key to Intercept Copyright Infringement

Sharanya K.R..[1], Nisha Saranga[2],Thashreefa[3], Naidile V.J.[4], Jayapadmini Kanchan[5]
[1,2,3,4] *Student, Department of Information Science engineering, SCEM, Mangaluru*
[5]*Professor, Department of Information Science engineering, SCEM, Mangaluru*

Abstract- **In Dynamic SLK (Software License Key) Management Using PK (Product Key) Generator, Software publishers have used digital rights management, specifically copy-protection techniques to prevent unauthorized and illegal copying of their software products. Common forms of prevention are copy protection techniques based on physical tokens. While physical tokens provide better protection from unauthorized copying than intangible ones, the protected digital content becomes unsuitable for online distribution. This project investigates the role of copy-protection techniques based on physical and intangible tokens in software piracy prevention using AES (Advanced Encryption Standard) Encryption Algorithm. Advanced Encryption Standard (AES) is used for increase data security and confidentiality. In this proposed approach data is encrypted. This project presents the general implications for a software publisher's anti-piracy and online distribution policy.**

Index Terms- **piracy ,serial key ,AES algorithm.**

I. INTRODUCTION

Today's P2P networks are grossly abused by illegal distributions of music, games, video streams, and popular software. These abuses have not only resulted in heavy financial loss in media and content industry, but also hindered the legal commercial use of P2P technology.

Traditional content delivery networks (CDNs) use a large number of surrogate content servers over many globally distributed WANs. The content distributors need to replicate or cache contents on many servers. The bandwidth demand and resources needed to maintain these CDNs are very expensive.

The main sources of illegal file sharing are peers who ignore copyright laws and collude with pirates. Copyright protection in P2P networks is an important issue. Many countries have passed the laws to protect digital copyrights. As a result, there were shutdowns of well-known websites (e.g., BT@China Union) and deletions of pirated contents (e.g., Mininova).

II. LITERATURE REVIEW

Many methods have been implemented for preventing copyright infringements based on different technologies. In this session is discussed about few of these works.

AES algorithm is used for data encryption and decryption, since it is faster and secure than any algorithm. This paper deals with different data security and privacy protection issues in a cloud computing environment and it provides different security services like authentication, authorization and confidentiality along with monitoring in delay. 128 bit Advanced Encryption Standard (AES) is used for increase data security and confidentiality.[1]

P2P helps to pirate copyrighted contents in the software product. The investigation on many important issues on the ways to prevent pirated content propagation in P2P networks. The system to stop pirated content propagation by utilizing several attacks to BitTorrent (BT) is developed[2]

There are many methods to secure software products from pirates such as water marking[3] , finger print technology[4],encryption[5] .

Decreasing the piracy without disturbing paid clients by sending unnecessary data i.e. poisonous chunks to violators. Client authorization Protocol (Cap) to differentiate unpaid clients from paid one's by assigning time stamp to copyright content file that can be downloaded by paid client exclusively[2]

Peer authentication Protocol (PaP) is used to enable clients to detect illegal download attempts from a pirate without communicating with a central authority[6]

Software splitting is a technique for protecting software piracy by removing code fragments from an application and placing them on a remote trusted server[7], peer has its own key and needs to purchase it for decryption. The study carried out in [17]

proposed a peer authorization protocol to distinguish illegal clients from legitimate ones.

The paper has done comparative study between different encryption methods like AES, DES and RSA based on analysis of simulation time for encryption and decryption. It concludes that AES algorithm is better than DES and RSA[9]

Table 1:Comparison between DES, RSA and AES algorithms

Features	DES	AES	RSA
Developed	1997	2000	1977
Key length	56 bits	128 ,192, 256 bit	More than 1024 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Asymmetric block cipher
Block size	64 bits	128 bits	Minimum 512 bits
Hardware & Software Implementation	Better in hardware than software	Better in both	Not efficient
Encryption and Decryption	Moderate	Faster	Slower

III.SYSTEM DESIGN AND IMPLEMENTATION

An architecture diagram is a representation of system design ,defines structure of process, behaviour, functionalities of all the components involved in the system. An architecture diagram of a system also gives the idea about the functional relationship between all components present in the overall system. An architecture diagram helps to understand the system.

For the proposed system, the architecture diagram is as shown in the figure. The proposed system is can be used by vendor when it is completely developed. Thus he/she become a authorized vendor and he can monitor the system. Viewing the authentication code from the system, adding product and

bank details to the system and generating serial key using this system are the functionalities of the vendor. The proposed system designed to fetch the 8 digit hard Disk ID and 8 digit processor ID of the system using management object searcher class and will produce an authentication code. Through this authentication code, a serial key will be generated. This unique serial key is given for products. This will be further encrypted. It can use 128, 192 or 256 bits of block size using AES Encryption algorithm for encryption. This unique product key which is generated by the vendor is given to the client. The client has to enter serial key in its field to purchase and use product. If entered serial key is belong to his PC it will be successful , then client can use the produt. Thus it will keep product safe from pirates.

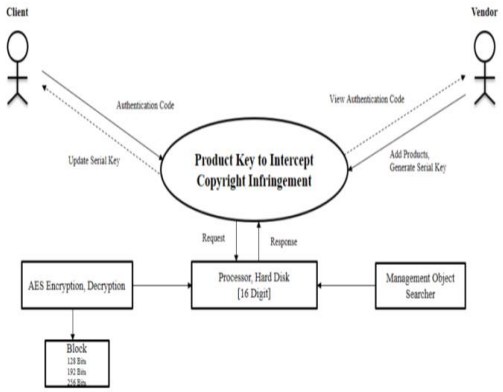


Fig: Architecture Diagram for Proposed System

Proposed system works on below pseudocodes

Login:
Input username, password.
If username exists then
Check whether password matches
If password matches then
Successful Login.
Else
Display error message
End if
Else
Display error message
End if

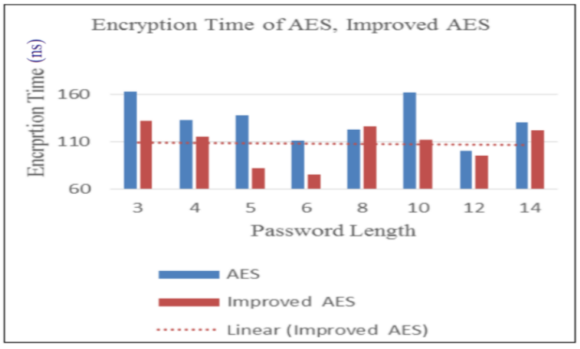
User Creation:
Input username, password, conform password ,user type, email, phone no.
Check if username exists
If exist then
Display error message
Else
Check if password and confirm password matches
If password matches then
New user created.
End if

Generate serial key:
Input authenticate code, bits , password
Check if password exist contains minimum 8 digits.
If true
Set authentication code, choose bits and apply password and generate serial key
Else
Display error message
End if.

AES Encryption:
Cipher(byte input[16], byte output[16], keyarray roundkey[Nr+1])
begin
byte statusarray[16];
statusarray = input;
AddTheRoundKey(statusarray, roundkey[0]);
for i = 1 to Nr-1 stepsize 1 do
Sub Bytes (statusarray);
Shift the Rows (statusarray);
Mix the Columns(statusarray);
AddTheRoundKey(state, round key[i]);
End for
Sub Bytes (statusarray);
Shift Rows (statusarray);
AddTheRoundKey(statusarray, round key[Nr]);
End

IV. RESULT ANALYSIS

The proposed project will prevent piracy of software products which is bought online.Hence it can be used for online distribution of software products. Every time the encryption takes place, the AES algorithm used here will make use of unique different keys. This unique key is generated by the technique used in the proposed system. It is analysed that the enhanced AES algorithm consumes less time compared to that of standard AES algorithm.



V. CONCLUSION AND FUTURE WORK

The Common form of preventing software piracy are copy-protection techniques based on physical tokens. Physical tokens are used to provide piracy protection from the unauthorized clients, but this method cannot be applied for online distribution of the software products. Hence as a result, the proposed project is well suitable for the online distribution of the software products which in turn will also prevent all the piracy issues happening worldwide. The techniques used in the proposed project works well in preventing the software piracies. Hence this method can be implemented by all the business companies which are involved in distributing the software products online.
The proposed project is an application which is designed in such a way that any further enhancements can be made easily. New modules as required by the client can be added easily to the existing system with least efforts. Future work for the proposed project aims at designing this system as mobile or IOS application as well.

REFERENCES

[1] Yawei Zhang, Lei Jin, Xiaojun Ye, Dongqing Chen, “Software Piracy Prevention: Splitting on Client”, 2008 International Conference on Security Technology, ISBN(p):978-0-7695-3486-2, 2008
[2] Vidya Waykule, Abhishek S Naswale, Rahul S Gaikwad, Mandar M Mahadeokar, Abhijit R Jain, ”Collusive Piracy Prevention in P2P Network”, International Journal of Advanced research in Computer Science and Software Engineering, ISSN:2277-128X, Vol-3, Issue-1, January 2013
[3] D. Tsolis, S. Sioutas, A. Panaretos, I. Karydis, and K. Oikonomou, “Decentralized digital content exchange and copyright protection via P2P networks,” in ISCC 2011, pp. 1056-1061, 2011. H. Simpson, *Dumb Robots*, 3rd ed., Springfield: UOS Press, 2004, pp.6-9.
[4] X. Li, S. Krishnan, and N. W. Ma, “A wavelet-PCA-based fingerprinting scheme for peer-to-peer video file sharing,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 365-373, 2010.

[5] Q. Qiu, Z. Tang, and Y. Yu, "A decentralized authorization scheme for DRM in P2P file-sharing systems," in Consumer Commun. Netw. Conf., pp. 136-140, 2011.

[6] Xiasong Lou, Kai Hwang, "Collusive Piracy Prevention in P2P Content Delivery Networks", IEEE Transactions on Computers, Vol-258, No-7, ISSN(p):0018-9340, February 2009

[7] Yawei Zhang, Lei Jin, Xiaojun Ye, Dongqing Chen, "Software Piracy Prevention: Splitting on Client", 2008 International Conference on Security Technology, ISBN(p):978-0-7695-3486-2, 2008

[8] Dr. Prerna Mahajan and Abhishek Sachdeva, Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security" Global Journal of Computer Science and Technology Network, Web & Security, ISSN(e): 0975-4172, ISSN(p): 0975-4350, Vol-13, Issue-15, 2013