Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Study on Securing Copyrighted Multimedia Data Using Double Encryption Technique to Prevent Piracy

Suraj Prakash*, Ashish Agarwal
MCA, VTU, Karnataka
India

Abstract— Entertainment world is the imagination of a huge era where unlimited music and movies are used to provide a feeling of personal satisfaction to the audience. Many people are involved in this field to make money as well as to earn fame with their hard work. But due to the lack of security and huge amount of data being generated, the hard work doesn't get its appropriate value. Data is being pirated in an unimaginable way. Viewers use them for entertainment while pirates use them for earning money from the hard work of the others. The money that pirates make belongs to movie director, producer and the entire cast and crew of a particular movie or song. But it does not reach to them because of the loopholes in this existing system. Hence, piracy prevention is the primary objective and focus of this paper. We propose a system where we use double encryption-decryption technique to prevent these activities in a large scale. Original data is encrypted using private key and then stored in the server. The encrypted data is again encrypted using public key before being sent through the network to the client. The doubly encrypted data is decrypted once by the client using the public key but the original data is decrypted only through the licensed media player, using the private key while playing the media file. Hence there is no such issue of data being stolen from the server.

Keywords— Cryptography, Encryption, Cloud based server, Diffie-Hellman, RSA, Doubly encryption technique.

I. INTRODUCTION

1. CRYPTOGRAPHY:

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. A cryptographic algorithm, also called a cipher, is the mathematical function used for encryption and decryption. (Generally, there are two related functions: one for encryption and the other for decryption.) If the security of an algorithm is based on keeping the way that algorithm works a secret, it is a restricted algorithm. Restricted algorithms have historical interest, but are woefully inadequate by today's standards. A large or changing group of users cannot use them, because every time a user leaves the group everyone else must switch to a different algorithm [1]. If someone accidentally reveals the secret, everyone must change their algorithm. The term is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption).

If we are taking about security of information then following services come in mind:

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)

SSL assures secure data transmission through the use of several security concepts [7].

A. History of Cryptography

There have been three well-defined phases in the history of cryptology.

1. The first was the period of manual cryptography, starting with the origins of the subject in antiquity and continuing through World War I. Throughout this phase cryptography was limited by the complexity of what a code clerk could reasonably do aided by simple mnemonic devices. As a result, ciphers were limited to at most a few pages in size, i.e., to only a few thousands of characters.
2. The second phase, the mechanization of cryptography, began shortly after World War I and continues even today. The applicable technology involved either telephone and telegraph communications (employing punched paper tape, telephone switches, and relays) or calculating machines such as the Brunsvigas, Marchants, Facits, and Friedens (employing gears, sprockets, ratchets, pawls, and cams). This resulted in the rotor machines used

by all participants in World War II. These machines could realize far more complex operations than were feasible manually and, more importantly, they could encrypt and decrypt faster and with less chance of error. The secure size of ciphers grew accordingly, so that tens or even hundreds of thousands of characters were feasible.

3. The third phase, dating only to the last two decades of the 20th century, marked the most radical change of all—the dramatic extension of cryptology to the information age: digital signatures, authentication, shared or distributed capabilities to exercise cryptology functions, and so on. It is tempting to equate this phase with the appearance of public-key cryptography, but that is too narrow a view. Cryptology's third phase was the inevitable consequence of having to devise ways for electronic information to perform all of the functions that had historically been done with the aid of tangible documents.

II. ENCRYPTION

Encryption is the process of conversion of data into a form, called a cipher text and so preventing any unauthorized recipient from retrieving the original data [9]. Many encryption algorithms are extensively available and used in information security. This is usually accomplished using a secret Encryption key and a cryptographic Cipher [13].
Two basic types of Encryption are commonly used:

- Symmetric Encryption, where a single secret key is used for both encryption and decryption.
- Asymmetric Encryption, where a pair of keys is used -- one for Encryption and the other for Decryption.

A. History of Encryption:

1. Scytale:

Introduced in 700 BC, The Spartan military used scytales to send sensitive missives during times of battle. Both sender and recipient had a wooden rod of the exact diameter and length. To encrypt a message, the sender tightly wound a piece of leather or parchment around the stick and wrote a message on it. The unwound leather was sent to the recipient, who could only read the message once it was tightly wound around his own scytale. Anyone else would see disarranged letters with no meaning.

2. Alberti Cipher:

In 1467, Leon Battista Alberti invented and published the first polyalphabetic substitution cipher, changing the course of encryption forever. The Alberti cipher was comprised of two metal discs on the same axle, one inside the other, which involved mixed alphabets and variable rotations.

3. Jefferson Wheel:

Invented by Thomas Jefferson in 1797, while he was George Washington's secretary of state, the wheel consisted of 26 cylindrical wooden pieces threaded onto an iron spindle. The letters of the alphabet were inscribed on the edge of each wheel in random order. Turning them would scramble and unscramble words. The recipient would spell out the coded message on his wheels and then look for the one line of letters that made sense. The U.S. Army used this encryption device again between 1923 and 1942.

4. Enigma machine:

Building on the work of Polish cryptanalyst in 1943, Bletchley Park- Britain's main decryption establishment during WWII - was set on decrypting the Enigma machine, a series of related electro-mechanical rotor cipher machines used by the Nazi military. It was considered unbreakable; as the Nazis changed the cipher every father of modern computing, Alan Turing, capitalized on the machine's one fundamental flaw: No letter could be encrypted as it. Armed with this information and Turing's Bombe machine, which greatly reduced the time required to crack Enigma, pretty soon the Allied forces knew the Wehrmatch's every move.

5. First Computer Password:

Developed by MIT's CTSS (computer Time Sharing System), when computer time was scarce, extremely expensive and limited to research institutions.In 1961, CTSS employed the first password and username method of user authentication-and may have been the first system to experience a password breach. In 1966, a software bug jumbled up the system's welcome message and its master password file, so that anyone who logger in was presented with the entire list of CTSS passwords.

6. DES:

The National Bureau of Standards invented DES (Data Encryption Standard) using state-of-the-art 56 bit encryption in 1979. At the time, it was so strong, not even super computers could crack it. Indeed, DES was the standard for almost 20 years – until the Electronic Freedom Foundation broke the DES key in 56 hours in 1998. A year later, they reduced that time to just over 22 hours.

7. Video cipher II:

HBO, Cinemax, and other began using a TV satellite scrambling system based upon DES called Video cipher II in 1985, making late-night watching of wavy-lined R-rated movies the pastime of an entire generation. A tremendous black

market emerged for descramblers, and six years after TV scrambling technology's debut, it was estimated that only 10% of dish owners were paying subscribers.

8. AES and CAPTCHA:

The National Institute of Standards and Technology developed AES (Advanced Encryption Standard) in 1997, which is still used today. 128-bit encryption takes 2 to the 55th power years to crack. A device that could check a billion (1018) AES keys per second (if such a device could ever be made) would in theory require about 3x10^51 years to exhaust the 256-bit key space.

As online spam grew, AltaVista chief Scientist Andrei Broder and his colleagues developed a filter that generated an image of random text that machine vision systems cannot read, though humans can. In 2009, Luis van Ahn at Carnegie Mellon updated the concept with extra layers of security that measured up to more evolved spam and hacking practices. With ReCAPTCHA, words became even harder for machines to read, thanks to increased waviness and features like lines running through the text.

9. Personal Data Lockers

Introduced in 2012 Personal data lockers have emerged as a way to make the most of the Internet while remaining safe. By centralizing storage of personal data—from payment information and passwords to ID numbers and receipts—in one locally-encrypted place that only the user can access, the data is as secure as possible, while remaining conveniently under his or her control. No one else can decrypt the data - not even the purveyors of the technology or the government can get to it. In a sense, personal data can grow go wherever a user wants it to go, but nowhere else [12].

10. SSL Encryption –

SSL is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL Connection. Both Netscape Navigator and Internet Explorer support SSL and many Web sites use the protocol to safely transmit confidential information, such as credit card numbers [7].

III. USED ARCHITECTURE – CLOUD SERVER

Cloud computing is originated from earlier large-scale distributed computing technology. NIST [8] defines Cloud computing as " a model for enabling convenient, on demand network access to a shared pool of configurable computing resources(e.g. , networks ,storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [6].

Use of cloud computing has evolved through a number of phases which include grid and utility computing, application service provision (ASP), and Software as a Service (SaaS). In order to ensure file security on cloud, the above cryptosystem is deployed on cloud. We assume cloud server as trusted but in order to prevent tampering/misuse of data by intruder or data leakage or other security concerns, the data is stored at server in the encrypted form.

Cloud Computing is a style of computing in which business provides application data and any type of IT resource as a services to client. To gain access to services of cloud computing you only need Internet access. Cloud computing is clearly one of today's most enticing technology areas due to its cost-efficiency and flexibility. But the overarching concept of delivering computing resources through a global network is rooted in the sixties [5].

The idea of an "intergalactic computer network" was introduced in the sixties by J.C.R. Licklider, who was responsible for enabling the development of ARPANET (Advanced Research Projects Agency Network) in 1969. His vision was for everyone on the globe to be interconnected and accessing programs and data at any site, from anywhere. "The most important contribution to cloud computing has been the emergence of "killer apps" from leading technology giants such as Microsoft and Google. Other key factors that have enabled cloud computing to evolve include the maturing of virtualization technology, the development of universal high-speed bandwidth, and universal software interoperability standards, said UK cloud computing pioneer Jamie Turner [15].

IV. EXISTING SYSTEM

With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, such as a time-sharing system, and the need is even more acute for systems that can be accessed over a public telephone or data network. The generic name for the collection of tools designed to protect data and to thwart hackers is computer security [11].

Film piracy refers to the act of stealing, copying, and distributing movies and other types of film. It is a major issue that has had major effects on the film industry and start-up production companies. Over the years there has been a tremendous decrease in DVD sales as a result of film pirating being so available.

Someone who goes online has the opportunity to commit film piracy. In fact, most Internet users will commit film piracy at some point while surfing the web. There are far too many resources for this to be done as well. You can find many peer to peer sharing programs such as torrent programs, and online movie streaming sites. All of which are forms of film piracy and by utilizing them you are breaking copyright infringement laws.

Film piracy is coined as being the act of copying and distributing film without permission from the copyright holder. This is a crime that many people commit even without noticing.

When film piracy first became very common it was mostly an issue of pirated movies being sold for a low cost. This influenced many individuals to purchase the pirated movies instead of buying the genuine copies of products from the stores at far higher prices. After peer-to-peer sharing programs and served based movie sites developed there was an even greater increase in film piracy. There have already been significant enhancements (increase) in the availability of pirated material over the past five years. Thus the copyright owners of the materials don't get the original value for their effort.

V. PROPOSED SYSTEM

The main feature of the encryption/decryption program implementation is the generation of the encryption key. Now a day, cryptography has many commercial applications. If we are protecting confidential information then cryptography is provide high level of privacy of individuals and groups. However, the main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation as described earlier [10].

Piracy of movies can be prevented if certain steps are taken and technology used in between. The movies are stored on a particular server where the data itself is stored in an encrypted form. Users must purchase an application called MV player which will have the decryption algorithm. Users can browse movies from this player and they can watch movies in real time. When the user requests for a particular movie, then the data which is already stored in an encrypted form, gets encrypted again on the server side and then it is sent to the user over the network. At the client side, the new encrypted data gets decrypted and stored in the MV player.

The MV player has the key to decrypt the original data. The data is decrypted using this application and the data is protected. Users are not allowed to save data at their terminal. They can watch the movie, if they want to watch it again, the same process is repeated. Using this way, we can preserve the original data from being transmitted over the network. The encryption technique which is used to store data at server is absolutely and obviously different from the encryption technique which is used to transmit the data over the network.

VI. WORKING OF PROPOSED MODEL

The movies are stored on a particular server where the data itself is stored in an encrypted form. While saving the data at the server, the data is encrypted using DHA algorithm (Diffie-Hellman technique) because this algorithm is very fast as well as very secure. The data that has to be stored at the server is of large volume. Hence, it has to be stored at the server. The Diffie-Hellman encryption technique is used for encrypting the original data and then the encrypted data is stored in the server. Diffie-Hellman uses a symmetric session key for encryption.

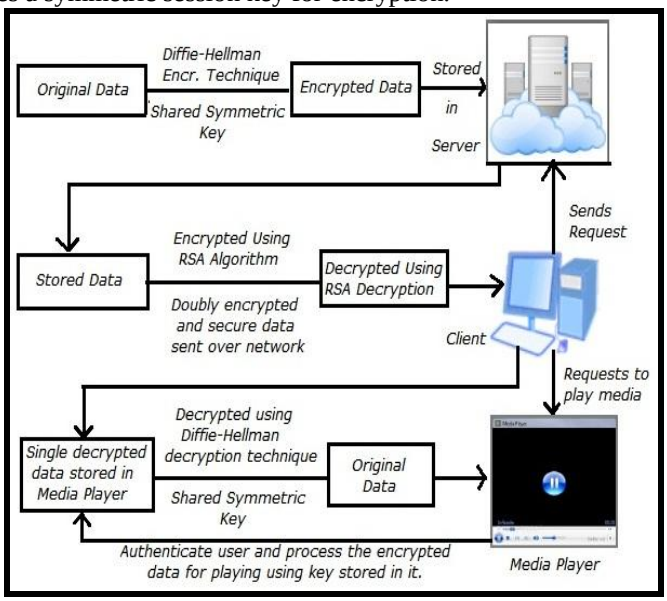

Figure-1 : Proposed Model

A. Diffie-Hellman (Existing Technique)

Diffie-Hellman was originally designed for key exchange. In the Diffie-Hellman cryptosystem, two parties create a symmetric session key to exchange data without having to remember or store the key for future use. They do not have to meet to agree on the key; it can be done through the Internet. This key can then be used to encrypt subsequent communications using a

1 RSA

1024 bits and above Fast Secure ---

2 DHA

1024 bits and above Very Fast Very Secure

Before establishing a symmetric key, the two parties need to choose two numbers p and g. The first number, p, is a large prime number on the order of 300 decimal digits (1024 bits). The second number is a random number. These two numbers need not be confidential. They can be sent through the Internet; they can be public [2].

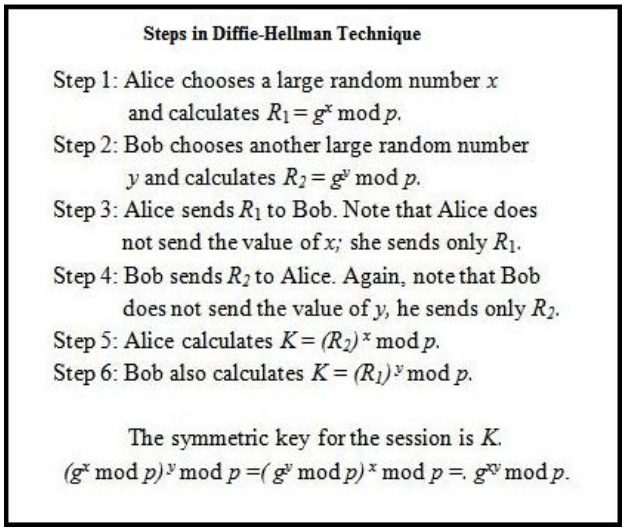

Figure-2 : Diffie-Hellman Steps

Bob has calculated K = $(R1)^y \bmod p = (g^x \bmod p)^y \bmod p = g^{xy} \bmod p$.
Alice has calculated K = $(R2)^x \bmod p = (g^y \bmod p)^x \bmod p = g^{xy} \bmod p$.
Both have reached the same value without Bob knowing the value of x and without Alice knowing the value of y.

The symmetric (shared) key in the Diffie-Hellman protocol: $K = g^{xy} \bmod p$.

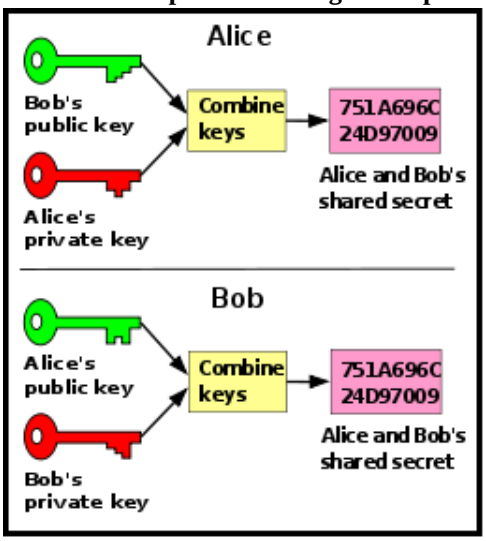

Figure-3 : Diffie-Hellman

Users must purchase an application called MV player which will have the symmetric shared key used in the above step to encrypt the original data. Using this key the media player can decrypt the encrypted data and the original data can be accessed. Users can browse movies from this player and they can watch movies in real time.
When the user requests for a particular movie, then the data which is already stored in an encrypted form, gets encrypted again using RSA algorithm on the server side and then it is sent to the user over the network. During transmission, data gets transmitted bit by bit and hence, we need not encrypt all the data at a time. It would be ideal to encrypt and send small data over the network which gets decrypted on the other side than to transmit whole data at a time.
At the client side, the new encrypted data gets decrypted using the RSA decryption technique and stored in the MV player. The MV player can decrypt the original data as discussed above. The data is decrypted using this application and the data is protected from piracy.

B. RSA (Existing Technique):

The most common public key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). Rivest-Shamir-Adleman is the most commonly used public key encryption algorithm. It can be used to send an encrypted message without a separate exchange of secret keys. It can also be used to sign a message [4].
RSA scheme is a block cipher in which the plain text and cipher text are integers between 0 and n-1 for some n. It uses two numbers, e and d, as the public and private keys. The two keys, e and d, has a special relationship to each other[3].

Steps in Selecting Keys in RSA

Step:1 Bob chooses two very large prime numbers p and q.
Step:2 Bob multiplies the above two primes to find n, the modulus for encryption and decryption. In other words, $n = p \times q$.
Step:3 Bob calculates another number $\phi = (p-1) \times (q-1)$.
Step:4 Bob chooses a random integer e. He then calculates d so that $d \times e = 1 \bmod \phi$.
Step:5 Bob announces e and n to the public; he keeps ϕ and d secret.

Figure-4 : Steps in selecting keys

Thus by using this double encryption-decryption technique the original data on the server will be protected from the pirates and the owners will also get the desired value for their hard work in creating the data [2].

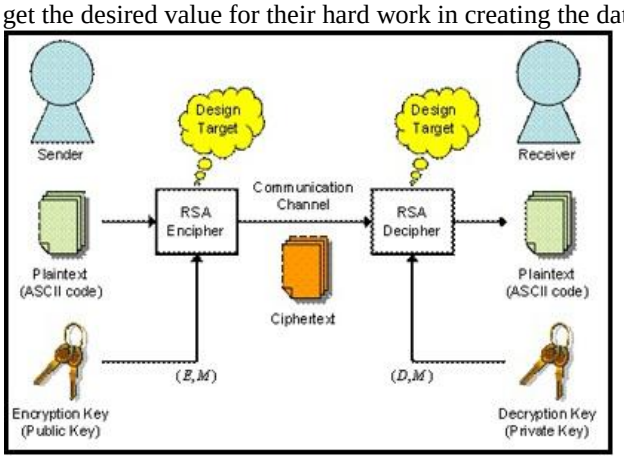

Figure-5 : Working of RSA Algoithm

VII. CONCLUSION AND FUTURE WORK

Piracy is a severe crime. By using this proposed system, piracy can be reduced to a great extent. It cannot stop the entire piracy that is being done in this modern world. As we are living in a technology driven world, there are several technology which are being used by the pirates to perform piracy of movies. Even though the original data is securely stored in the server and only the authorized user can access it and view it as many times as they want using the MV player. But still there are several possibilities of making piracy, using HD cameras with good resolution capacity while watching the movie is one of the ways.

There are certain areas in this system which needs to be improved. The data can be sent more securely to the client by using virtual private network, where there is very less chance of facing problems such as data loss and network traffic. This VPN will improve the transfer speed of the data as traffic in the PVN is not much as compared to the public network. Precautions can be taken in movies theatre to prevent piracy by using advanced technology like Camera detectors, mobile phone detectors etc which can be used by the pirates to make a pirated version of the original movie being played inside the hall. The cinema halls must use CCTV cameras to identify the pirates who bring cameras or any other electronic devices. The above application can also be used for other applications and in sensitive areas where we need to handle confidential data which must not be lacked at any cost.

REFERENCES

[1] B. Schneier, Applied Cryptography, 2ed. John Wiley and Sons, 1996.
[2] Behrouz A Forouzan, Data Communications and Networking, 4th Edition, The McGraw-Hill Companies.
[3] E. Ramraj and S. Karthikeyan,"A new type of network security protocol using hybrid encryption in virtual private networking", Journal of Computer Science 2, 2006 Science Publications.
[4] Pradeep Kumar Panwar, Devendra Kumar, " Security through SSL", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012.
[5] Pankaj Patidar and Arpit Bhardwaj, "Network Security through SSL in Cloud Computing Environment", International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011.
[6] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", NIST, 2010.
[7] Philip, R., M. Bellare and J. Black,"A block-cipher mode of operation for efficient authenticated encryption". ACM Trans. Information System and Security, OEM, 2003.

[8] Reema Gupta, Tanisha, Priyanka, "Enhanced Security for Cloud Storage using Hybrid Encryption", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013.
[9] Srinivasarao D et al., "Analyzing the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011.
[10] Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance cryptography algorithm for improving data security ",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.
[11] William Stallings, Data and Computer Communications, 6e William 6e 2005.
[12] www.britannica.com/EBchecked/topic/145058/cryptology/25637/History-of-cryptology.html
[13] www.hitachi-id.com/concepts/encryption.html
[14] www.visual.ly/history-encryption.html
[15] www.computerweekly.com/feature/A-history-of-cloud-computing.html
[16] www.researchgate.net/publication/221609728_OCB_a_block-cipher_mode_of_operation_for_efficient_authenticated_encryption.html

