International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 11 Issue 2, February, 2022, Impact Factor: 7.751

Implementation of Round Robin Keys for enhancement of Data Security

Prity Kumari[1], Dr. Upendra Kumar[2]

[1]Mathematics Department (Computer Science), Magadh University, Bodh Gaya, India
[2]Birla Institute of Technology, Patna

ABSTRACT

Today entire world is looking towards digitalization, so very complex data scrambling technique demands in today era for data security. This technique is much equivalent to our shadow whenever any person sees our shadow, they can't identify person. Likewise, when attacker see our encoded message then scrambled message seen as a shadow mode and they can't understand it. Today many enhanced Cryptography technique comes to scramble data but it is not enough, therefore I tried to implement new concept provide more security for transmission of data in network and that technology inbuild in OSI layer. As we know each layer of OSI protocol play important role for secure data transmission between one device to another. In this paper more than one secret key use for data scramble and those keys are getting from OSI layer. In this paper we give detailed explanation of getting port number, session ID, IP address and MAC address as a security key. These keys are switches between themself by key switching technique and applying RC4 encryption Technique to encrypt data. All keys are changeable/renew during transmission time and key switching take place between them in some time interval through timer thus, this technique known as "Round Robin keys switching (RRKS) technique".

Keywords-OSI Model; Session ID; MAC Address; IP Address; Port Number; Key Switching; RC4; Timer

INTRODUCTION

Over the past twenty years, all organization has utilized theOpen System Interconnection (OSI) Model for better connectivity of hardware and software [4]. The Open System Interconnection (OSI) model characterizes a network framework to use protocols in seven layers. It partitions network communication into seven layers. Networks work on one fundamental principle: "pass it on". Every layer deal with a quite certain activity for securely transmit data, afterward passes the information onto the subsequent layer. In OSI layer, control passed from starting i.e. application layer than onto the next layer [1].

Very enhance technology are coming for transmitting datasafely in OSI layer, so many complex keys are using to scramble data but it is not much sufficient. For enhancement of security to transmit message between these layers, use more than one keys to encrypt data. In this paper more than one keys just like port number, session ID, IP address, and MAC address are used for encode data and that keys comes between these OSI layers. To make more complicated technique use key switching technique to change key frequently in certain time interval through timer. To make very complex security,all keys are also changeable for example session Id renew whenever any privilege level changed occurs during the user session, IP address changes when new port added or removed, the changes in MAC address depend on an interface such as Wi-Fi interface, LAN interface and Port number change whenever our request change.
Each application will have a port number related to it. A port number is a 16-bit unsigned integer and its range is from 0 to 65535. Specific port numbers are reserved to recognize definite services so that an arriving packet easily forwarded to a consecutively application.

In computer network if the server must realize who are you, it needs an approach to distinguish you each time you demand a page. It does that by utilizing session IDs. Session IDs utilized for an assortment of reasons; however, their principle object to permitted web designers to make different kinds of intelligent sites. For example, if engineers have made a protected domain, they might need to force visitors to go through the home page first. Or on the other hand, the engineers may need an approach to continue an incomplete session.

The session ID can save as a cookie, form field, or URL (Uniform Resource Locator). Cookies *can* high secure then URL, since they aren't something that ordinary users can copy and paste, or even view and modify. They're a more secure default. Encrypted cookies basically more complex. they're bigger in size, they need a complex algorithm, they necessitate that algorithm to properly implemented, they do contain real information and are along these lines' worth

attacking, they do want the management of a secret key. They're likewise harder to revoke because of their decentralized nature. Some session id is generated through simple method just like incrementing static number but some are generated through algorithm that include more complicated method just like use different variable along with factoring date and time of visit [2].

A session key may derive from a hash value, using the *Crypt Derive Key* function. The Crypt Derive Key function produces crypto graphical session keys derivative from a base data value. This method uses MD5 hash function called a *session-key derivation scheme*. Session keys are in some cases called *symmetric key*s, because the similar key utilized for both encoding and decoding that sent through network. At whatever point the sender wants to direct a protected information to the receiver, and after creating the communication session, this session ID of the receiver's computer recite by the encoding technique to utilized it as a key to encode the information.

At the point when our PC linked with a network, it allocated an address on the network called an IP address. It's a network address for our port so the Internet realizes where to send you messages, information and pictures.IP (Internet Protocol) Addresses is unique logical address for all systemcontain four octal numbers. The range of each number in between 0 to 255 [3]. Suppose a system on the network have an IP address 12.110.11.15 and the system beside it have an address 12.110.11.16. Routers is a device to forward message from one computer to another with the help of its IP address [4].

These four parts of the IP address formed to represent a vector (chromosome) of 4 bytes. For example: (12:110:11:15) is represent (in Hexadecimal) as: A:48:9:D

IP address is combining with port number to give us a socket. There are many different port numbers for different protocol. For example:-**12.110.11.15:80**

Where 12.110.11.15 is IP address and 80 is port number of http protocol.

In this paper instead of IP, utilizesIPsec cryptographic security to enhance secure communications over Internet Protocol (IP) networks. All types of application verified through IPSec. It provides information confidentiality, integrity, birthplace verification etc over the network [5].

Network Interface Cards (NIC) exists in data link layer to enable ports to converse with one another. So, to communication they assigned a one single physical network address called Media Access Control (MAC) Addresses. ARP (Address Resolutions Protocol) utilized to map MAC address from IP address of any system[6].

Rivest cipher 4(RC4)algorithmswere named on developerRon Rivest in 1987. Today it is widely acceptable due to its simplicity.This is stream cipher scheme totally based onXOR operation on a stream of data and that data is in form of bytes.The encryption in RC4 is done by XORing plaintext and keystream. XORing is done between packets byte by byte to generate cipher data.RC4 encoding and decoding speed is very high in comparison to other technique [7].

RELATED WORK

Writer Dr. Mohammed Abbas Fadhil Al-Husainy describe the functionality of MAC address in OSI layer protocol. MAC address assigns a single physical address recognizes PCs individually on network at moderately layer 2. In this paper, author recommended encoding method use MAC address as a key for encoded data. MAC address utilized to verify the recipient system just like computer, mobile and all devices linked with network. This system was tried on certain information, visual and numerical estimations were utilized to check the quality and execution of the strategy. Thisresearch demonstrated the proposed procedure utilized effectively to scramble information that transmitted throughnetworks [8].

In this paper author Angel Yu, Wai Lok Lai, James Payor gives Homomorphic Encryption yields intentionally flexible ciphertext, permitting tasks on encrypted information. They introducedtoapply homomorphic encoding scheme for encodes integer vectors to permit calculation of random polynomials in the encodedfield with a limited stepproposed by Zhou and Wornell. This discoveryis especially applying in cloud computation.When data is transmitted through system then adapting low dimensional representations of dataare stored in scrambled form[9].

To enhancements ofall previousidea, Tragha, A., Omary, F., and Mouloudi, A.create new concept from the combination of cryptography techniqueby genetic algorithm named as ICIGA that is improved cryptography integrated by genetic algorithm. In this method author use session key for encode data and that session key is generated form irregular method by ICIGA algorithm. User can fix key length and block size but in starting phase the size of block and the length of key is varies. It is improved technology of GIC that is genetic algorithm inspired cryptography [10].

In this paper author describe Session id used as Encoding data and Session Tracking accommodated Apply two

streaming method that is HTTP Live Streaming (HLS) and Microsoft HTTP Smooth Streaming (HSS) Adaptive Bit Rate (ABR) protocols.ABR streaming method provide high quality streaming method for live or pre-recorded content transmitted through HTTP server in the network.DRM schemes provide more security attachwithcontent and continue attach, no matter where to move content or what to do with it. This scheme is different from access restrictions from other placed withcontent once it is transmitted. It supported by the service provider, givesoutcomes in high storage limit both inside the definitive store just as the Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS) cache order. Session-Based Encryption can intensely decrease on the whole storage requirements [11].

PROPOSED TECHNIQUE

Data file (message/plaintext) transmitted frequently in OSI treated as a set of N bytes and arrange it into packet. Throughout the processes the port number of sender and receiver, RC4 encryption algorithm, session Id, IP address of host and destination, and MAC address transmitted along with each message available during the transmission process of OSI model. These all keys obtained from different OSI layers. In these key session Id renew whenever any privilege level changed occurs during the user session, IP address changes when new port added or removed, the changes in MAC address depend on an interface such as Wi-Fi interface, LAN interface and Port number change whenever our service/request change.A different session key may get for every time by getting from session cookie. A Timer used to switch the key. If in timer we set 100ms time to switch the key for message and when time is over then next message go to next key for encryption and so on. This switching technique does work like round robin for switching keys to encrypt messages, so it's called **round robin keys switching technique.**

Below are steps to transmit message with attach keys in different layer:

1) Message Mdistributed through application layer with source and destination port number defined as P_S and P_D.
$$((M) + P_S,P_D)$$
2) In Presentation Layer Message translated, compressed and decoded through SSL/TLS protocol.
$$((M+P_S,P_D)+RC4)$$
Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic security protocols. They're utilized to protect network. Their primary objectives to given information integrity and message security. RC4 applications are used in SSL and TLS. RC4 is simpler encryption technique and so it is used in various applications.
3) In Session Layer we get Session ID and merge with it.
$$(((M+P_S,P_D),RC4)+SID)$$
4) In Transport Layer Message divided into segment.
$((M1+P_S,P_D,M2+P_S,P_D,M3+P_S,P_D$ …… $),RC4,SID)$
In this layer message divided into small segment and every segment carries segment sequence number and source and destination port number.
5) In network layer Multiple segment divided into packet with source and destination IP address but we use Secure IP(IPSec).
$$((M1+IPSec_S,\ IPSec_D,M2+IPSec_S,\ IPSec_D,M3+IPSec_S,\ IPSec_D$$ …… $) ,P_S,P_D,RC4,SID)$$
6) In data link layer Packet divided into frames with MAC address.
$$(((M1,M2,M3$$ …… $),IPSec_S,\ IPSec_D,\ P_S,P_D,RC4,SID)+MAC)$$

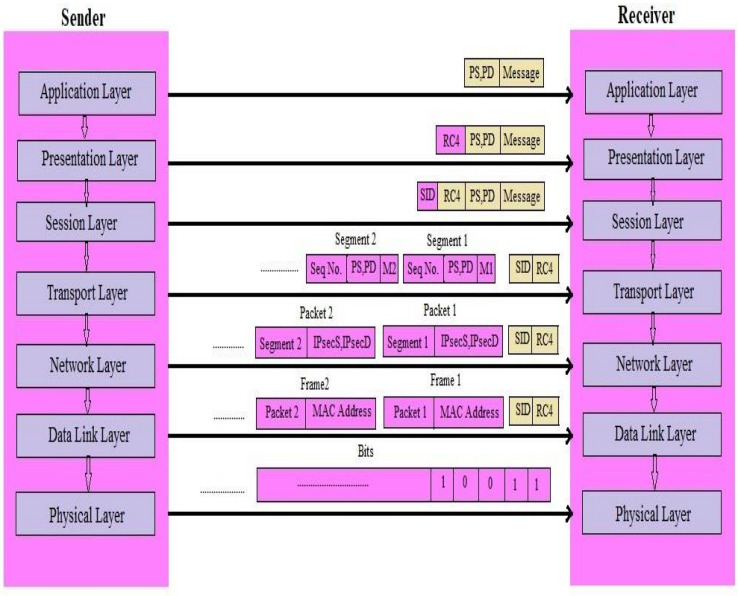

Fig. 1. Layer of OSI Model to Select Multiple Key

A. Key Switching

Key switching is the technique to change multiple keys during message encryption in after some interval. Key switching permits changing a secret-key–ciphertext while encoding the original plaintext. When plain text transmitted into a network in the form of small packets that packets will go through key switching technique.If suppose a message divided into 10 packages, and in timer set50ms time to switch the next key, then after 50ms next packet will encrypt by next key arrange in proper sequence. If time is over to encrypt 9^{th} packet then 10^{th} packet will encrypt with next secret key arrange in a proper key sequence and if at a same time user request next job then that job will also be divided into packets and resume previous secret key and start encryption process and so on. As we will see, key switching rearranges the execution and completion of large number of our tasks.

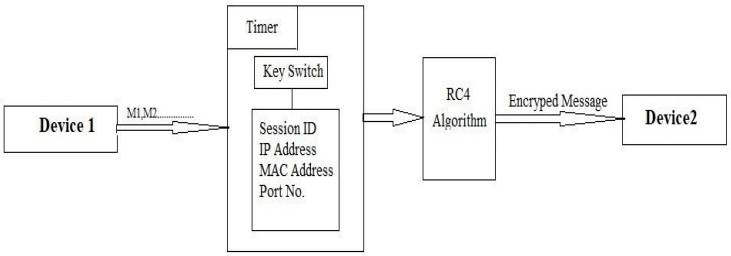

Fig. 2. Key Switching Technique

B. Timer

The timer is electricalpass having quite an output (with or without contact) which electrically closes (turns ON) or opens (turns OFF) the circuit after a preset time passes by when electrical or mechanical information is given.

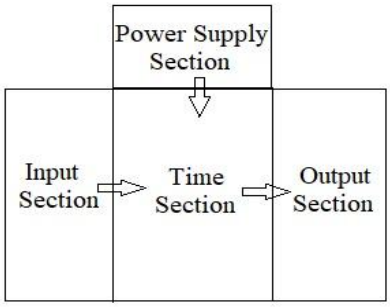

Fig. 3. Timer

In the above timer machine, power supply section supplied the applied voltage to the internal component, input section receive signal from sender and output the signal to the time section, time section measures the time setting and output a signal to the output section at specific time setting in timer and output section give output signals to receiver. Two function indicators indicate the timer status that is such as Power indicator and Output indicator. The power indicator measures the power is being supplied or not in the timer whereas output indicator sees the status of the output.The functioning mode determines the output technique that utilized whenever the set time has reached. A fixed time interval defines on the timer, when time has reached then key automatically sift on the next defined key [12].

C. RC4

In thistechnique use multiple keys get from sevenlayer of OSI. Thesekeys are use as secret key to encrypt data.

Encryption:

1) User inputs a text message and multiples of keys like session ID, IP address, MAC address and port number.
2) RC4 encoding engine produce keystream by selecting one key between them.
3) Now this keystream XOR with text message and XORing is done byte by byte to generate cyphertext.

Decryption:

1) To decrypt the cyphertext message, receiver is also doing XOR between cyphertext and same keystream.

CONCLUSION

This paper presents an effective method for message encoding which employs the round robin keys switching technique. The main purpose of a key switching is to improve security against surveillance, eavesdropping, malware, spyware, and theft of IoT devices. Port number, Session IDs, IP address and MAC address of the sender and receiver

machine to use as a key for encoding. Switching keys apply to successfully communicate secretively in a network. This security technique is better than all existing technique because all keys change frequently and switching between them also. One key does not fix to encrypt data every time, so it provides high security. If anyone stolen one key, then they cannot decrypt all data because keys changes for encrypt next data for very small time. This procedure made a decent invulnerability for the information that communicated through networks. Thus, the proposed round robin keys switching technique provides a more secure and convenient technique for secure data transmission for OSI model.

REFERENCES

[1]. Webopedia "The 7 layer of OSI model", http://www.Webopedia.com/quickref/OSI_Layers.asp (June1, 2004)
[2]. "SessionID"https://searchsoftwarequality.techtarget.com/definition/session-ID(Jan2006)
[3]. Tsutsumi, Toshiyuki**, "**Secure TCP providing security functions in TCP layer", April29,2004, URL: http://www.isoc.org/HMP/ PAPER /144/html/paper.html, (June 1,2004)"Introduction to SSL", October 09, 1998, http://developer.netscape.com/docs/manuals/security/sslin/contents.htm, (June 1,2004)
[4]. Osterloh, Heather. "ITCP/IP Addressing and the protocol suite" CCNA2.0 Prep Kit 640-507Routingand Switching Indianapolis, Indiana, USA: Que, 2000.(Ch6)
[5]. Norton, Peterand Stockman, Mike. "Network Security Fundamentals" First Edition. Indiana polics, Indiana, USA: SAMS, 2000.(Ch1,p15)
[6]. "ARP"http://compnetworking.about.com/library/glossary/bldef-arp.htm(01 Mar.2002).
[7]. https://www-geeksforgeeks-org.cdn.ampproject.org/v/s/www.geeksforgeeks.org/what-is-rc4-encryption/amp/?amp_js_v=a6&amp_gsa=1&usqp=mq331AQHKAFQArABIA%3D%3D#aoh=16078379083513&referrer=https%3A%2F%2Fwww.google.com&amp_tf=From%20%251%24s&ampshare=https%3A%2F%2Fwww.geeksforgeeks.org%2Fwhat-is-rc4-encryption%2F
[8]. Zhou, Hongchao, and Gregory Wornell. "Efficient homomorphicen cryptio non integer vectors and its applications." Information Theory and Applications Workshop (ITA). IEEE,2014.
[9]. AngelYu, WaiLokLai, James Payor" Efficient Integer Vector Homomorphic Encryption" https://courses.csail.mit.edu/6.857/2015/files/yu-lai-payor.pdf, (14 May2015)
[10]. Tragha,A.,Omary,F.,andMouloudi,A.,"ICIGA:Improvedcryptographyinspiredbygeneticalgorithms". International Conference on Hybrid Information Technology (ICHIT'06). pp. 335-34,(IEEE,2006).
[11]. AppendixF"ABR Session-Based Encryption and Session Tracking" https://www.cisco.com/c/en/us/td/docs/video/cds/cda/is/4_3_3/configuration_guide/SCG1/ABRsessionEncryption.pdf
[12]. "Technical Explanation for Timers and Time Switches" CSM_Timer_Timeswitch_TG_E_7_3, https://www.ia.omron.com /data_pdf/guide/19/timer_timeswitch_tg_e_7_3.pdf