Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 6, June 2016, pg.41 – 47

Enhancement of Wireless Network Security by Customized Encryption Technology & using Multilayer of Security

Sonu[1], Surender Singh[2]

[1]Computer Science & Engg. Department, Om Institute of Technology & Management, Haryana, India
[2]Assistant Professor, Computer Science & Engg. Department, Om Institute of Technology & Management, Haryana, India
[1] soniajhajhria11@gmail.com, [2] surender.punia@yahoo.com

Abstract - Wireless computing proposes new ways to provide services. These pioneering technical & pricing opportunities bring changes within way business operated. Lack of security is only barrier within wide adoption of cloud computing. The rapid growth of Wireless computing has brought many security challenges for users. Wireless computing offers many benefits, but it also is vulnerable to threats

Keywords – "Cryptography, IP Filter, RSA, AES, OTP (One Time Password), Java"

I. INTRODUCTION

A **wireless network** is any type of computer network which is using wireless data connections to connect network nodes. Wireless networking is a method by which domestic, telecommunications networks & enterprise installations avoid costly process of introducing cables in a building. Because a connection among different equipment locations. Wireless telecommunications networks are generally implemented & administered using radio communication. Such implementation takes place at physical level of Open System Interface model network structure. The examples of wireless networks consist of cell phone networks, Wireless local networks, wireless sensor networks, satellite communication networks, & terrestrial microwave networks.

- ***Terrestrial microwave*** – Terrestrial microwave communication usually make utilization of Earth-based transmitters & receivers resembling satellite dishes. Terrestrial microwaves are within low gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately forty eight km (thirty mi) apart.
- ***Communications satellites*** – Satellites communicate via microwave radio waves, which are not deflected by Earth's atmosphere. The satellites are stationed within space, typically within geosynchronous orbit 35,400 km (22,000 mi) above equator. These Earth-orbiting systems are capable of receiving & relaying voice, data, & TV signals.
- ***Cellular & PCs systems*** - Cellular & PCS systems make use of make several radio communications technologies. The systems divide region covered into multiple geographic areas. Every area has a low-power transmitter or radio relay antenna device to relay calls from one area to next area.

- ***Radio & spread spectrum technologies*** – Wireless local area networks use a high-frequency radio technology is same as digital cellular & a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication among many devices within a limited area. IEEE 802.11 defines a common flavor of open-standards wireless radio-wave technologies are known as Wifi.
- ***Free-space optical communication*** - uses for visible or invisible light for communications. In most cases, line-of-sight propagation is used, which limits physical positioning of communicating devices.

II. Types of Wireless Networks

Wire-less PAN

Wireless is a personal area networks interconnect devices within a relatively small area, that is comely with a person's reach. example, both Bluetooth radio & invisible infrared light provides a WPAN for interconnecting a headset to a laptop. ZigBee also supports WPAN applications. Wi-Fi PANs are becoming common place as equipment designers are starting to integrate Wi-Fi into the variety of costumer electronic devices. Intel My Wi-Fi & Windows seven virtual Wi-Fi capabilities have made Wi-Fi PANs simpler & easier to setup & configure.

Wireless LAN

Wireless Land area networks is often used for connecting to local resources & to Internet A wireless local area network (WLAN) links are two and more than two devices over short distance using a wireless distribution method, usually providing a connection by an access point for internet accessing. The use for spread-spectrum or OFDM technologies could allow the users to move within a local coverage area, & still remain connected to network.

Products using IEEE 802.11 WLAN standards have been marketed under the brand name of Wi-Fi. Fixed wireless technology implementation point-to-point links among computers/networks at two locations at different places, often using for dedicated microwave/ modulated laser light beams over line of sight paths. It is often used within cities to connect networks within two/more buildings without installing a wired link.

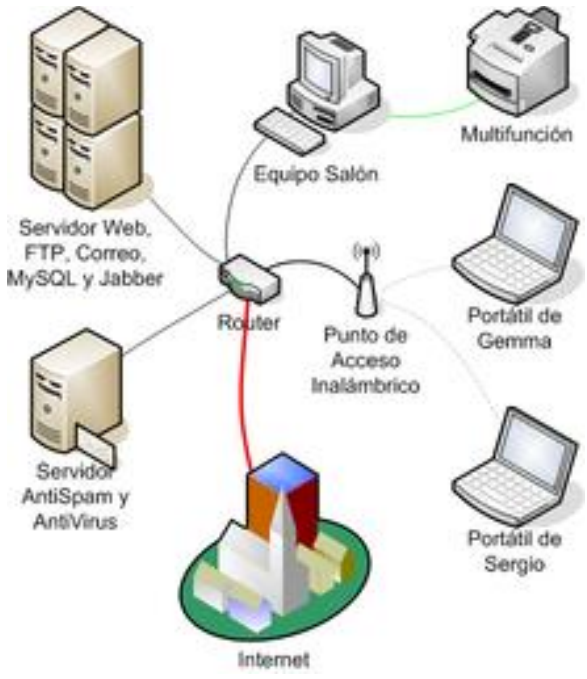

Fig 1. Wireless Local area Network

Wireless Land area networks is often used for connecting to local resources & to Internet A wireless local area network (WLAN) links are two and more than two devices over short distance using a wireless distribution method, usually providing a

connection by an access point for internet accessing. The use for spread-spectrum or OFDM technologies could allow the users to move within a local coverage area, & still remain connected to network.

Products using IEEE 802.11 WLAN standards have been marketed under the brand name of Wi-Fi. Fixed wireless technology implementation point-to-point links among computers/networks at two locations at different places, often using for dedicated microwave/ modulated laser light beams over line of sight paths. It is often used within cities to connect networks within two/more buildings without installing a wired link.

Wireless mesh network :-

Wireless mesh network is wireless network made up for radio nodes organized within a mesh topology. Each node forwards messages on behalf of other nodes. Mesh networks could self-heal, automatically re-routing a node which has lost its power.

Wireless MAN

Wireless metropolitan area networks are a type of wireless network which would connect several wireless LANs.WiMAX is a type of Wireless MAN & is described by IEEE 802.16 standard.

Wireless WAN

Wireless WAN is wireless network is that typical covered large areas, like between neighbouring towns & cities, or city & suburb. These networks could be used to connect branch offices of business or as a public internet access system. Wireless connections among access points are usually point to point microwave links using parabolic dishes on 2.4 GHz band, rather than omni directional antennas used with smaller networks. A typical system consists of base station gateways, access points & wireless bridging relays. Other configurations are mesh systems where every access point acts as a relay also. When combined with renewable energy systems like photovoltaic solar panels or wind systems they could be stand alone systems.

Global area network

A global area network is used for supporting mobile across a arbitrary are number of the wireless LANs, satellite coveraged areas, etc. The key challenged with in mobile network is handing off user communications from one local coverage area to next. In IEEE Project 802, this consists of a succession of terrestrial wireless LANs.

Space network

Space networks are networks used for communication between spacecraft, usually within vicinity of Earth. Example of this is NASA's Space Network.

III. Problem Statement & Objectives

There was problem with existing security system. There was security threat by crypto analyst. Crypto analyst is person who could access convert encrypted data to decrypted form using this cracking techniques.Lack of security is only barrier within wide adoption of cloud computing. The rapid growth for cloud computing have buy more security challenges for users. Cloud computing offers many benefits, but it also is vulnerable to threats. One of main threat exist today is problem of unauthorized users or entities. For avoiding this problem new technique is developed within this cloud computing is that data owners could share their outsourced data with a large number of users, who might want to retrieve certain specific data files they are interested within during a given session.

The main objective of research is to secure the data by integrating IP filter and OTP mechanism to enhance the security of cryptography based wireless network.

IV. Existing Implementation

Cryptography

***Encryption Steps*:-**

- Encryption of plaintext that is to be send by sender use to encryption from secret picture which can actually sender's private key & thus generating cipher text using DES.
- Further, it would carry out process on secret picture by use of covered picture which is receiver's public key & thus encrypting with in Rivers Shamir Adleman algorithm for example RSA.
- A digital envelope is sent to receiver having cipher text & picture so encrypted.

***Decryption Steps*:-**

The Decryption of message received from sender's side would occur as follow:

- Digital envelope would reach receiver's side.
- Digital envelope would be opened to get encrypted picture & decrypt using its own private key with RSA algorithm & receiver get secret picture.
- Cipher text would be changed using planet extusing secret picture applying DES.
- Thus receiver would get plain text.

Socket implementation after Cryptography

Here we would create our server & client communication protocol using own port using socket programming.

1. **First step is to create server side port using following algorithm**

- Create ServerSocket object using our own port 6666.
- Accept client request using Server socket object.
- Receive data from client within form of input data stream object.
- Convert data stream object to string
- Input data stream is within form of cipher data decrypted are using proposed algorithem.
- The Close Connection

2. **Second step is to create Client side interface to connect to server.**

- Create ServerSocket object using our own port 6666 to connect to server
- Encrypt data before sending.
- Send data using data output stream object.
- Clean output buffer.
- Close connection.

V. PROPOSED MODEL

In proposed model there would be triple layered security:-

1. Security layer 1 would be customized cryptography algorithm of AES to enhance security.
2. Security layer 2 would drop packets from unauthentic IP addresses.
3. Security layer 3 would authenticate user by providing login password security at application layer.
4. Security would be enhanced using one time password also that becomes useless after using one time.
5. In this way we will secure wireless network from external attacks and authentic access.

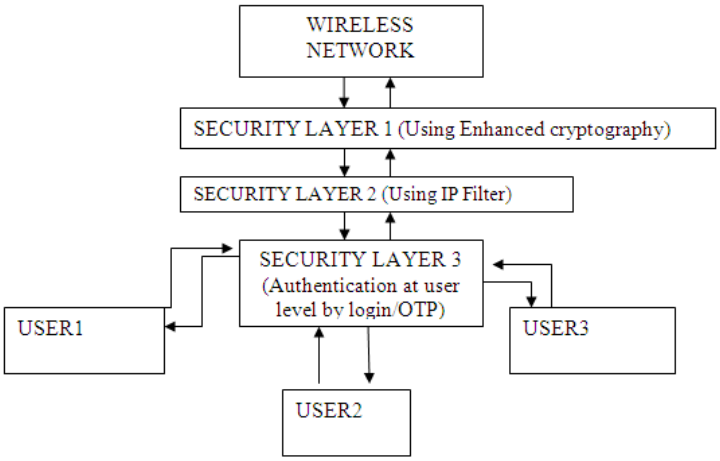

Fig. 2 Triple Layer Security

OTP GENERATION

One time password would be generated randomly by Math.random() function in java. Each and every time the complex OTP number could be generated to be used during decryption.

Using Math.random() double random = Math. random() * 50 + 1; or int random = (int)(Math. random() * 50 + 1); ...

Using Random class in Java. Random rand = new Random(); int value = rand.nextInt(50); This will give value from 0 to 49. For 1 to 50: rand.nextInt(50) + 1.

IP Filter

Centralized database of IP address would be created on centralized server and decryption request from authentic IP would be accepted. If IP is not found in database or its status is 0 then Decryption would not be allowed.

VI. Tables and figures of transmission speed of Packets in different media:-

Sr. No	Security_Level	H	L	Avg
1	Layer1(cr)	20	40	30
2	Layer2(ip)	15	30	22.5
3	Layer3(otp)	10	20	15
4	L1+L2	40	80	60
5	L1+L3	35	70	52.5
6	L2+L3	30	60	45
7	L1+L2+L3(slow_ net)	55	110	82.5
8	L1+L2+L3(avg_n et)	50	100	75
9	L1+L2+L3(High_ net)	48	96	72
10	L1+L2(avg_net)	45	90	67.5
11	L1+L3(avg_net)	40	80	60
12	L2+L3(avg_net)	35	70	52.5

Table 1 Data in case of Fiber optics cable

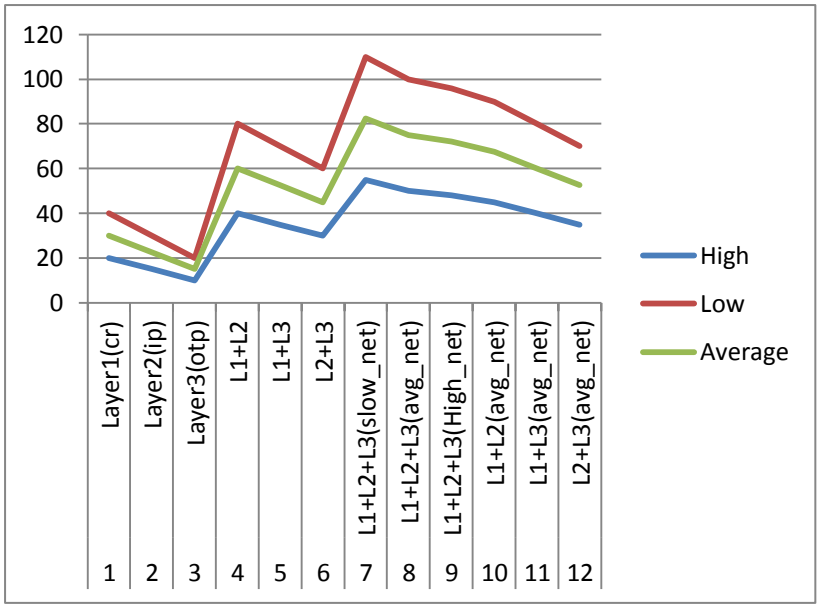

Fig 3. Analysis of transmission speed of packet in case of Fiber optics cable

Sr.No.	Security_Level	H	L	Avg
1	Layer1(cr)	25	50	37.5
2	Layer2(ip)	20	40	30
3	Layer3(otp)	15	30	22.5
4	L1+L2	45	90	67.5
5	L1+L3	40	80	60
6	L2+L3	35	70	52.5
7	L1+L2+L3(slow_net)	60	120	90
8	L1+L2+L3(avg_net)	55	110	82.5
9	L1+L2+L3(High_net)	53	106	79.5
10	L1+L2(avg_net)	50	100	75
11	L1+L3(avg_net)	45	90	67.5
12	L2+L3(avg_net)	40	80	60

Table 2 Data in case of Coaxial Cable

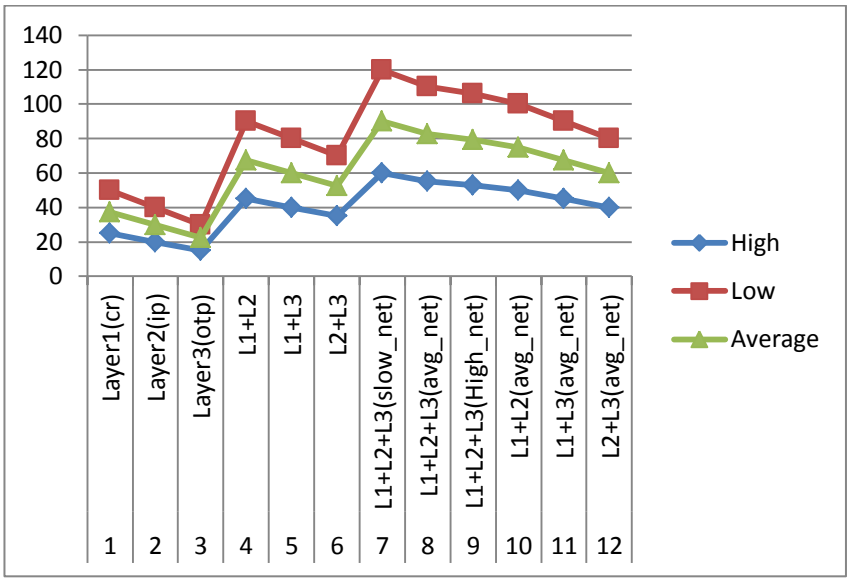

Fig 4. Analysis of transmission speed of packet in case of Coaxial Cable

Sno	Security_Level	H	L	Avg
1	Layer1(cr)	30	60	45
2	Layer2(ip)	25	50	37.5
3	Layer3(otp)	20	40	30
4	L1+L2	50	100	75
5	L1+L3	45	90	67.5
6	L2+L3	40	80	60
7	L1+L2+L3(slow_net)	65	130	97.5
8	L1+L2+L3(avg_net)	60	120	90
9	L1+L2+L3(High_net)	58	116	87
10	L1+L2(avg_net)	55	110	82.5
11	L1+L3(avg_net)	50	100	75
12	L2+L3(avg_net)	45	90	67.5

Table 3 Data in case of Twisted Cable

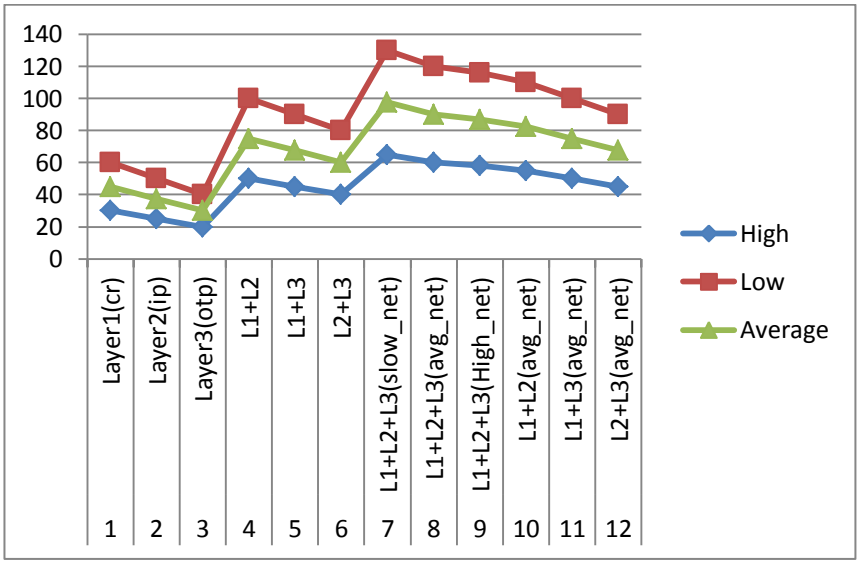

Fig 5 Analysis of transmission speed of packet in case of Twisted Cable

Sr. No	Security_Level	H	L	Avg
1	Layer1(cr)	35	70	52.5
2	Layer2(ip)	30	60	45
3	Layer3(otp)	25	50	37.5
4	L1+L2	55	110	82.5
5	L1+L3	50	100	75
6	L2+L3	45	90	67.5
7	L1+L2+L3(slow_net)	70	140	105
8	L1+L2+L3(avg_net)	65	130	97.5
9	L1+L2+L3(High_net)	63	126	94.5
10	L1+L2(avg_net)	60	120	90
11	L1+L3(avg_net)	60	120	90
12	L2+L3(avg_net)	50	100	75

Table 4 Data in case of Wireless Network

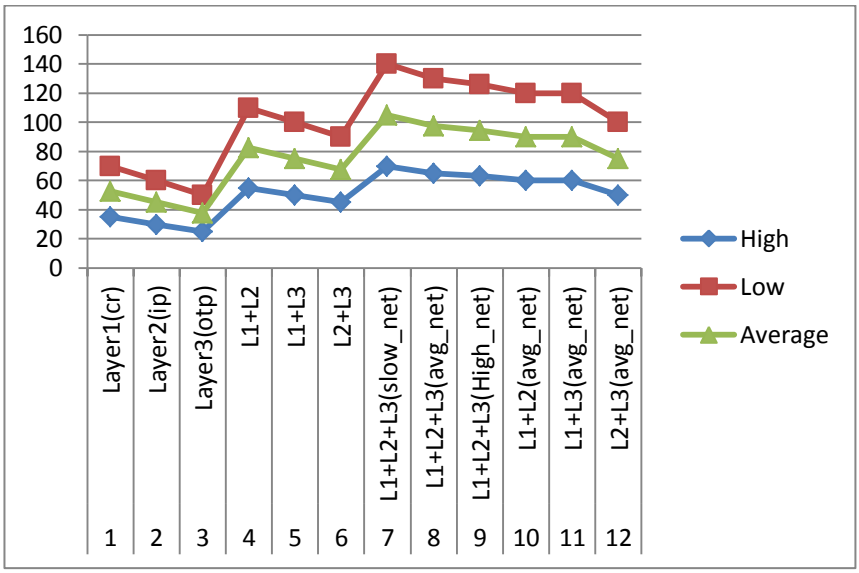

Fig 6 Analysis of transmission speed of packet in case of Wireless network

VII. Conclusion & Future Scope

We have enhanced security by enhancing encryption algorithm. Here we have also defined our own ports for server and client. Its defined new rules for encryption & decryption & involved multiple layer of security like IP Filter & OTP code this would definitely improve security mechanism within Wireless computing environment.

Future Analysis could be made on different network and topology. Additional security layers may be added to enhance security

References:

1. Natasha Saini1, Nitin Pandey2, Ajeet Pal Singh3," Enhancement Of Security Using Cryptographic Techniques", 978-1-4673-7231-2/15©2015 IEEE.
2. Bhushan Chaudhari, Prathmesh Gothankar, Abhishek Iyer, D. D. Ambawade,"Wireless Network Security Using Dynamic Rule Generation of Firewall", 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20,2012.
3. Raghav Mathur, Shruti Agarwal," Solving Security Issues in Mobile Computing using Cryptography Techniques -A Survey", International Conference on Computing, Communication & Automation (ICCCA2015), ISBN:978-1-4799-8890-7/15©2015 IEEE.
4. Sangita A. Jaju, Santosh S. Chowhan," A Modified RSA Algorithm to Enhance Security for Digital Signature", 978-1-4799-6908-1/15©2015 IEEE.
5. Natasha Saini1 ,Nitin Pandey2, Ajeet Pal Singh3," Enhancement Of Security Using Cryptographic Techniques", 978-1-4673-7231-2/15©2015 IEEE.
6. Michael Ekonde Sone," Efficient Key Management Scheme to Enhance Security-Throughput Trade-off Performance in Wireless Networks", Science & Information Conference 2015 July 28-30.
7. Takahiro Fujita, Kiminao Kogiso, Kenji Sawada, & Seiichi Shin, "Security Enhancements of Networked Control Systems Using RSA Public-Key Cryptosystem", 978-1-4799-7862-5/15©2015 IEEE.
8. Prachi, Surbhi Dewan, Pratibha, Comparative Study of Security Protocols to Enhance Security over Internet", 2015 Fifth International Conference on Advanced Computing & Communication Technologies, 2327-0659/15© 2015 IEEE.
9. Antonio F. Skarmeta, Jos´e L. Hern´andez-Ramos, M. Victoria Moreno, "A decentralized approach for Security & Privacy challenges in Internet of Things", 2014 IEEE World Forum on Internet of Things (WF-IoT). 978-1-4799-3459-1/14©2014 IEEE.
10. Yasmin Alkady, Mohmed I. Habib, Rawya Y. Rizk," A New Security Protocol Using Hybrid Cryptography Algorithms", 978-1-4799-3370-9/13©2013 IEEE.

