International Journal of Research in Advent Technology, Vol.7, No.4, April 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Implementation of Algorithm to Protect Data from Different Attacks at Application Layer

Pooja Dahiya[1], Sonal[2]
Student, M.Tech (CSE), B.P.S.M.V., Khanpur Kalan, Sonipat (131305), Haryana, India[1]
Assistant Professor, Department of CSE & IT, B.P.S.M.V., Khanpur Kalan, Sonipat (131305), Haryana, India[2]
Poojadahiya902@gmail.com[1],sonalkharb@gmail.com[2]

Abstract*:* Network security is mechanism that is providing authorization to user to access the resources remotely. But there are several threats to existing network security. This paper present the implementation of algorithm used to protect data from different type of attacks at application layer. Security is a major concern for safe communication between mobile nodes in an alien environment. Network security has considered the authorization of access to information that is transferred over network. This information has been managed by network administrator. It is becoming significant to users as well as companies. Firewall is forcing to access policies in such a way that users could access services after getting authentication. After development & testing of proposed work, comparative analysis between existing & proposed work have discussed the security mechanism at application layer.

Keywords: Network Security, Application Layer, Data Protection, IDS, Cryptography

1. INTRODUCTION

Network security provides authorization with username as well as password. The Network security consists of provisions policies. These policies have been adopted by a network administrator. The objective is to monitor and prevent misuse and unauthorized access. It also restricts alteration in system, or denial of computer resources that could be accessed over network. Network security considers the authentication information access that is transferred over network. This transmission is managed by network administrator. Security is significant for users and companies [1] that work on network. Firewall is forcing to access policies in such a way that users could access services after getting authentication. Because to check unauthentic entry to system. Such element may be unable to restrict computer worms or Trojans. These are transmitted on the network. The Antivirus software or IDS is helping to detect malware [2]. Communication among nodes that are utilizing a network could use cryptography in order to set the privacy policy.

2. RELATED WORK

In this section a review of various researches made by different authors has been made. Some authors have made a review on password cracking strategies and password stealing attacks & its protecting mechanism. Some of them discussed Identity Based Attack Detection and Localization by Clustering in Wireless Sensor Network. Several researchers have discussed security issues in protocols of TCP/IP Model at Layers Level and presented a review on Data Security, challenges and research Opportunities. Many of them explored database security and did study on threats & attacks. Benefits as well as limitation along with techniques discussed by researcher present in table (1).

Table 1 -Chart of existing researches

Sr No	Auth-or	Year	Technique	Benefits	Limitations
3	Bhawan Bhardwaj et al.	2017	Ad hoc network	Provide security for packet sniffer, brute force, man in middle, ip spoofing, ip level security.	Does not provide security for intrusion detection
4	Albandari Mishal Alotaibi et al.	2017	TCP/IP Model	Security issues in Protocols of TCP/IP Model at Layers Level have been resolved.	Does not provide solution for denial of services.
5	Ganesh Shankar Pote et al.	2016	Database security	Study made on Threats & Attacks on Database Security.	Focus on database only.
6	Tuhin Das et al.	2016	Clustering in Wireless Sensor	Identity based attack	Threat from intrusion

			Network	resolved	detection
7	Amandeep Kaur et al.	2016	Wireless Sensor Network	Provide security to wireless sensor network	Requirement to upgrade the security
8	Venkadesh .S et al.	2015	Password Stealing Attacks	Security to password has been proposed	Threat from denial of services
9	E Bertino et al.	2014	Data Security	Data Security – Challenges and Research Opportunities have been discussed.	Need of more technical work.
10	Amandeep Kaur et al.	2014	Mobile Ad-hoc Networks	Provide security to mobile ad-hoc network	Requirement to enhance the security
11	Ms. Vidya Vijayan et al.	2014	Password Cracking Strategies	Strong password mechanism has been proposed	There is still threat of brute fource attack
12	Ashwini R. Tonde et al.	2014	Encryption Standard Algorithm	Security during data transmission has been enhanced.	Research does not provide solution for packet dropping.
13	Mukund R. Joshi et al.	2013	Cryptography	Enhancement of network security using cryptographic	Does not provide solution in case of ping of death
14	Rupam, Atul Verma et al.	2013	Packet Sniffing	Provide security for packet sniffer and man in middle attack	Does not provide security for brute force , intrusion detection
15	Wajeb Gharibi	2012	Cyber threats	Provide security	Does not provide
	et al.			for intrusion detection	security for brute force , packet sniffer
16	Mr. Atul M. Borkar et al.	2011	AES Algorithm	Strong encryption mechanism has been proposed	Need to provide security from packet sniffer attack
17	Shahriar Mohammadi et al.	2011	Link Layer	Provide security for man in middle attack	Does not provide security for packet sniffer, brute force ,

3. PROPOSED WORK

Proposed work is enhancement of security system in order to protect from different attacks at application layer. There is requirement to develop a server & client application in order to secure data at application layer. Encoded data is transmitted to client at receiver end decoded data is captured.

3.1 Existing Algorithm

The process of encryption utilizes a group of particularly derived keys called round keys. The following steps were taken to encrypt a one hundred twenty eight bits (128bits) block [18].

Step1: Cipher key generate by the group of round key.
Step 2: Set the condition array within block data.
Step3: Join first key to beginning state array.
Step4: Perform Copy operation of final state array out as encrypted data.

3.2 Bit Shifting Process Along With Xor Operation

S'1, C=63⊕ ({02}.CO) ⊕ ({03}.FE) ⊕9C
({02}.CO)=11000000<<1 (1 Shift to the left)
=10000000
10000000⊕00011011=10011011
(xor ed with "00011011" because lost high bit of 1 in the shift)
({03}.FE)=11111110<<1
=11111100
11111100⊕00011011=11100111
(xor ed with "00011011" because lost high bit of 1 in the shift)
11100111⊕11111100=00011011
63=01100011
9C=10011100

10011011⊕00011001⊕01100011⊕10011100=01111101= 7D

3.3 Proposed Algorithm

ALGORITHM AT SENDER END

The steps of proposed algorithm at sender end are as under:-

Step 1: Internet Protocol filter has been utilized to ignore the invalid packet transmission from server to client. If packet is valid then enhanced AES ENCRYPTION module works. This step restricts the intruder.

Step2: In this step enhancement of network security is done by modifying present encryption mechanisms.

The working of AES at sender end is as following:-

I. TAKE PLAIN TEXT (256 bits)
II. APPLY ROUND KEY set counter=1
III. If counter is less then N-1 (Here N would be number of iteration)
   a) Process sub byte.
   b) Perform Shift row
   c) Mix columns
   d) counter=counter+1;
IV. other wise
   a) Sub bytes process
   b) Then row shift
   c) Then round key apply
V. Cipher text would be generated (256 bits)

Step 3: Perform Data Transmission

ALGORITHM AT RECEIVER END

The steps of proposed algorithm at receiver end are as under:-

Step 1: Receive the data.

Step 2: Perform decryption of data at receiver end

i. TAKE CIPHER TEXT (256 bits)
ii. APPLY ROUND KEY set counter=1
iii. if counter is less then N-1
   a) Process Inverse shift row.
   b) Perform inverse sub byte
   c) Inverse mix columns
   d) Counter=counter+1;
iv. other wise
   a) Inverse shift rows
   b) Inverse sub byte
   c) Apply round key
v. Plain text would be generated (256 bits)

3.4 Comparison Of Existing Algorithm With Proposed Work

In case of existing work there was security of data at application layer only. Due to limitation of existing security mechanisms there was need to develop a new security system. In proposed work security has been provided to packet and chance for decryption without authentication should get reduced. There is need to implement IP filter based security in order to prevent attacker from different network would enhance Advanced Encryption Standard by introducing multilayer security.

Brute Force attack is removed in the proposed algorithm as data is transferred during specific session. Attacker who is using brute force attack would not be capable to detect when then port to receive data has been opened on receiver end**.**

3.5 Process Flow

The process flow of proposed work has been discussed in following diagram. Here sender generated packet is transferred for IP validation. If packet is arriving from valid IP then drop packet and stop otherwise packet would be encrypted and transmission is made. On receiving end the data would be decrypted and plain text would be provided to receiver.

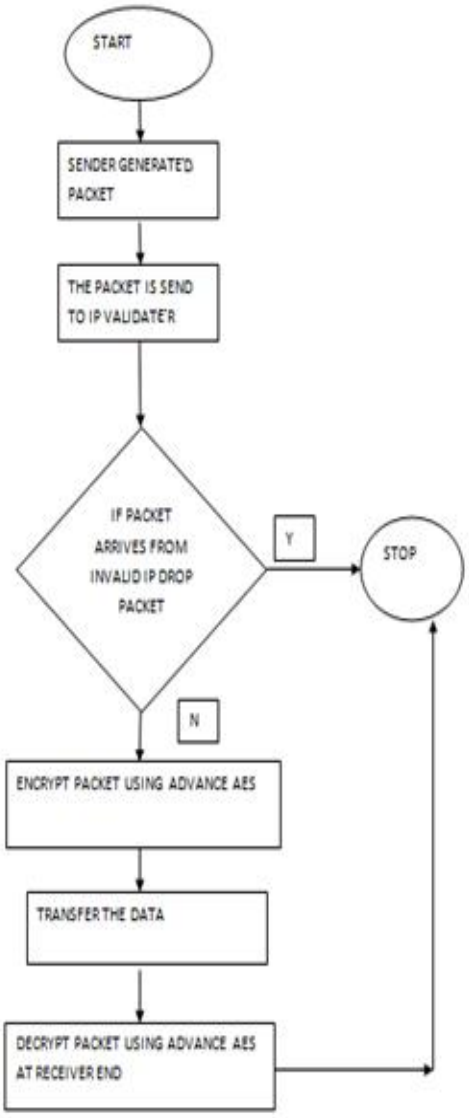

Fig 1: AES at sending and receiving end

4. RESULTS

GUI INTERFACE FOR CLIENT

This is the file sender interface that would send data to the server. Here the user id, password, port number, IP address, path of file to be send along with security token and AES CODE**.**

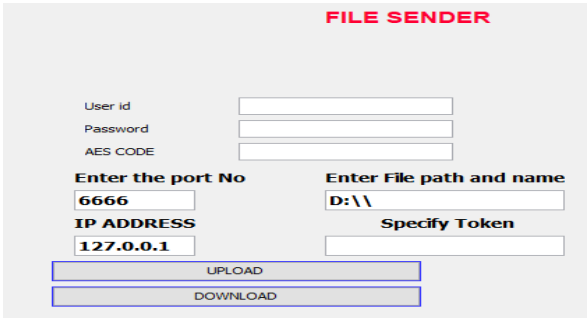

Fig 2: Sender Side Application

GUI INTERFACE FOR SERVER

This is the file sender interface that would send data to the server. Here the port number, AES CODE, path of file to be received along with security token.

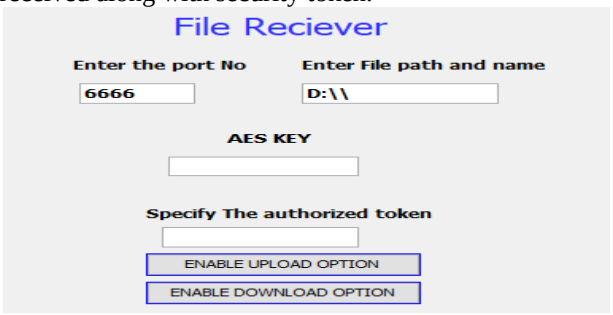

Fig 3: Receiver side Application

FILE FOR TRANSFER

Following file would be transferred to the receiver from sender end. It may be notepad file.

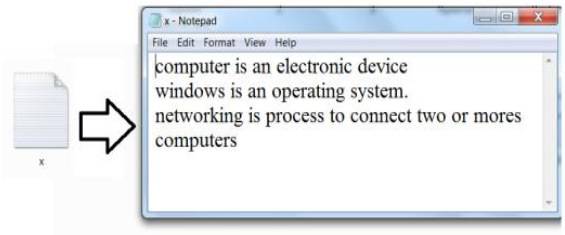

Fig 4: Transfer for File

FILE RECEIVED

Following file would be received at the receiver end. The content of that file would be same as file sent from sender end**.**

Fig 5: File Received

ENCRYPTED FILE

Here we have represented the content of file during transmission. It is cipher text that is not readable. If any person is going to hack that information then he would be unable to understand it.

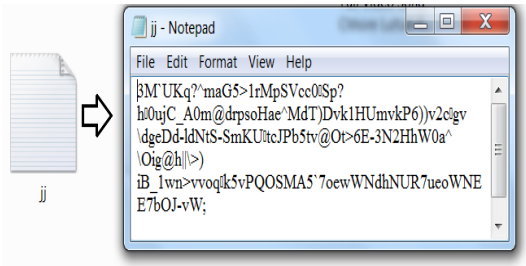

Fig 6: Encrypted File

4.1 Getting Data for Simulation

The simulation of data transmission result in following data:-

PACKET DROPPING

Packet dropping table (2) has been generated by considering the difference between packet sent and packet received during above java based packet transmission simulation.

Packet dropping= Packet sent-Packet received

TIME TAKEN TO TRANSFER DATA

Time taken to transfer data table (3) has been generated by considering the difference between receiving time and sending time during above java based packet transmission simulation. Time taken to transfer data is calculated by following equation

Time Taken= Receiving time-Sending time

ERROR RATES

Error rate has been influenced by packet dropping table (4) generated during above sending receiving data transmission module. It is influenced by several factors such as type of data, size of data, transmission media, number of processes, technical issues.

Error Rate= Number of Errors / Number of Packets

PACKET SIZE

The size of packet has been reduced during encryption in order to reduce the chances of congestion and errors. This table (5) has been generated during above sending receiving data transmission module.

4.2 Simulation in Matlab Introduction To Matlab Tool

The simulation has been made in MATLAB 2018 b. MATLAB is mathematical laboratory. Here the simulation is made by collecting data from java based socket programming in text file and MATLAB script have been written to plot diagram. Here MATLAB functions such as plot, hold on, title, x label, y label, legend have been used. MATLAB GUI tools have used for simulation.

COMPARATIVE ANALYSIS OF PACKET DROPPING IN EXISTING AND PROPOSED WORK

When data is transferred over network there is always probability of attack and packet dropping. Here the comparison of packet dropping in case existing and proposed work has been made.

Table: 2 Packet dropping in existing and proposed work

Packets	Existing	Proposed
100	5	3
200	9	3
300	10	4
400	12	4
500	14	7
600	18	8
700	30	12
800	40	23

Following is MATLAB based chart plotted to represent the comparative analysis of packet dropping between existing and proposed work.

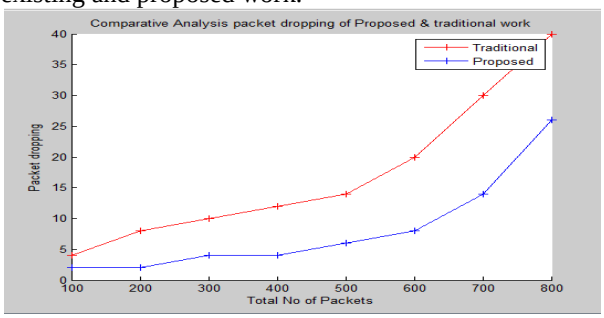

Fig 7: Comparative Analysis of Packet Dropping in Existing & Proposed work

The above figure shows comparative analysis packet dropping in case of existing & proposed work.

COMPARISON OF TIME TAKEN IN ORDER TO TRANSFER DATA

Following chart represents the time taken during transmission of data in case of existing and proposed work. This chart represents that the time taken are less as compare to existing work. Here the simulation is made considering packet size of 10, 20, 30, 40, 50, and 60 respectively.

Table 3- Comparison of time taken to transfer data

Packets	Existing	Proposed
10	1	0.7
20	1.7	1.5
30	2.3	1.7
40	2.8	2.4
50	3.8	2.9
60	4.8	3.4

Following is MATLAB based chart plotted to represent the comparative analysis of time taken between existing and proposed work.

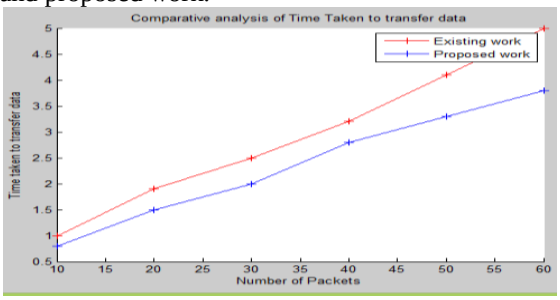

Fig 8: Comparison of Time Taken to Transfer Data

The above figure shows comparative analysis in case of existing & proposed work. Details of time taken to transfer packet have been compared here.

THE COMPARISON OF ERROR RATES DURING TIME OF TRANSFER DATA

Following chart represents the error rates during transmission of data in case of existing and proposed work**.** This chart represents that the error rates are less as compare to existing work. Here the simulation is made considering packet size of 10, 20, 30, 40, 50, and 60 respectively.

Table: 4 Comparison of error rates during time of transfer data

Packets	Existing	Proposed
10	1	0.6
20	1.5	1
30	2.1	1.6
40	2.6	1.8
50	3.9	2.5
60	4.2	3.5

Following is MATLAB based chart plotted to represent comparative analysis between existing and proposed work.

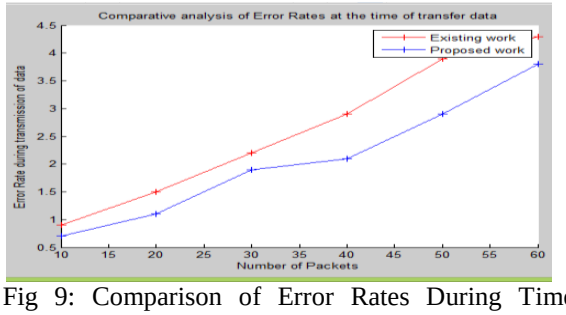

Fig 9: Comparison of Error Rates During Time of Transfer Data

This figure shows comparison of error rates during time of transfer data during existing & proposed work.

COMPARISON OF PACKET SIZE

Following chart represents error rates during transmission of information in case of existing and proposed work**.** This chart represents that error rates are less as compare to to existing work. Here simulation is made considering packet size of 10, 20, 30, 40, 50, and 60 respectively.

Packets	Existing	Proposed
10	10	7
20	14	10
30	18	15
40	28	17
50	32	25
60	41	30

Table 5- Comparison of packet size

Following is MATLAB based chart plotted to represent comparative analysis between existing and proposed work

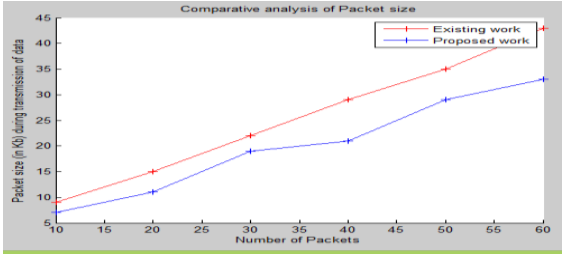

Fig 10: Comparison of Packet Size

This figure is displaying comparison of packet size in case of existing as well as proposed work.

5. FUTURE SCOPE

The results of work show that in case of secure transmission speed of data transmission is reduced if length of packet is minimized. The speed of data transmission may increase in contrast of secure existing work if packet size is reduced. With the expansion of internet, the security of network is gaining attention increasingly. The protocols of security threats of internet were examined to decide which type of security technology is required. Security technology is mostly based on the software. It uses many general hardware devices. The development in today's time in Security of network is not considerable. Hence proposed work would play important role in enhancing security of data.

REFERENCES

[1] M. Malik, T. Patel, "Database Security - Attacks and Control Methods", International Journal of Information Sciences and Techniques (IJIST) Volume.6, No.1/2, March 2016,pp.175-183.

[2] D. Andriy, P. Gulia, "Critical Review of Security Attacks in Wireless PAN", International Journal of Computer Applications, Volume 160 – No 1, February 2017,pp.15-19.

[3] B. Bhardwaj, A. Mittal, "Advanced Mechanisms to Secure Wireless ad hoc network with performance Analysis", Volume: 08 Issue: 08, October - December 2017.

[4] A. M. Alotaibi, B. F. Alrashidi, S. N. Z. Parveen, "Security issues in Protocols of TCP/IP Model at Layers Level", International Journal of Computer Networks Communications Security, Volume. 5, No. 5, May 2017, pp. 96-104.

[5] G. S. Pote, A. Giri, "Database Security: A Study on Threats & Attacks", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 4 Issue: 6, June 2016, pp. 512 – 513

[6] T. Das, "A Study on Identity Based Attack Detection and Localization by Clustering in Wireless Sensor Network", International Journal of Computer Sciences and Engineering Open Access, Volume-04, Issue-02, Feb 2016, pp. 96-99.

[7] A. Kaur, S. S. Kang, "Attacks in Wireless Sensor Network- A Review", International Journal of Computer Sciences & Engineering, Volume.04, Issue 05, May 2016, pp.157-162.

[8] Venkadesh .S, K. Palanivel , "A Survey on Password Stealing Attacks & Its Protecting Mechanism", International Journal of Engineering Trends & Technology (IJETT) , Volume 19, Number 4 , Jan 2015, pp.223-226.

[9] E. Bertino, "Data Security – Challenges and Research Opportunities", Springer International Publishing Switzerland, 2014, pp. 9–13.

[10] A. Kaur, Dr. A. Singh, "A Review on Security Attacks in Mobile Ad-hoc Networks", International Journal of Science & Research, Volume 3, Issue 5, May 2014, pp.1295-1299.

[11] V. Vijayan, Ms. J. , Mrs. Suchithra , "A Review on Password Cracking Strategies", International Journal of Research in Computer & Communication Technology, 2014, pp.8-15.

[12] A. R. Tonde , A. P. Dhande, "Implementation of Advanced Encryption Standard (AES) Algorithm Based on FPGA", International Journal of Current Engineering and Technology, Vol.4, No.2 April 2014, pp.1048-1050.

[13] M. R. Joshi, R. A. Karkade, "Network Security with Cryptography", International Journal of DDOS Attack Using Time series Analysis", Journal of Control Science & Engineering,2013, pp.1-6.

[14] Rupam, A. Verma, A. Singh, "An Approach to Detect Packets Using Packet Sniffing, International Journal of Computer Science & Engineering Survey (IJCSES) ,Volume.4, No.3, June 2013, pp.21-33

[15]W. Gharibi, M. Shaabi, "Cyber threats in social networking websites", International Journal of Distributed & Parallel Systems (IJDPS), Volume.3, No.1, January 2012, pp. 119-126.

[16] Atul, M. Borkar, R. V. Kshirsagar, M. V. Vyawahare, "FPGA Implementation of AES Algorithm", IEEE, 2011, pp.401-405.
[17] S. Mohammadi, R. E. Atani, H. Jadidoleslamy, "A Comparison of Link Layer Attacks in Wireless Sensor Networks", Journal of Information Security, April 2011, pp. 69-84.
[18] Anju, Babita, Reena, A. Aggarwal ,"An Approach to Improve the Data Security using Encryption and Decryption Technique", International Journal of Information and Computation Technology, Volume 3, Number 3, 2013, pp. 125-130.