IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A COMPARATIVE ANALYSIS OF DIFFERENT FIREWALLS WITH PROPOSED HYBRID IP FILTER AND PORT FILTER BASED FIREWALL

[1]Mr. Akshat Rana, Reseach Scholar, Department of Electronics Engineering, BMU, Rohtak-124001
[2]Dr.Anil Dudy, Associate Professor, Department of Electronics Engineering, BMU, Rohtak-124001

Abstract:

In the work we are taking into consideration the element of distance over time, as well as throughput and energy usage. In the investigation that has been suggested, data have been sent from sender to receiver in a format that is compressed, and an IP filter has been used to block the transmission of data that is not legitimate. The use of a firewall within the framework of the suggested technique offers protection on many different levels. Encryption has been used in order to make certain that the data is kept in a secure environment, and session security makes it possible for users to initiate a session even when data is in the process of being transferred. IP filters deny access to Internet Protocol (IP) addresses that have not been previously validated. A user-defined port number, which is included as part of the multilayer firewall security, enables the user to make use of a customized protocol. This ability is made possible by the firewall. It has been shown that variables such as speed and distance have a significant impact on the length of time required, the quantity of energy that is used, and the throughput.

Introduction:

Present research paper considers 4 firewalls in integrated manner to improve the security.

IP Filter

IP stands for "Internet Protocol," and it is an address that is used exclusively for identifying a system. The data connection from an authentic system is taken into consideration by the IP filter. The incoming request from an unauthentic system is disregarded by the IP filter. Therefore, a connection of an authentic system is possible thanks to the firewall's IP filter.

Port Filter

The port filter takes into account the genuine port. The port numbers that come before 1024 have been set aside for future use. The number of user-defined ports is more than 1024. During the process of initializing a connection, the port on the receiving end is the one that is initialized. The sender is only permitted to transmit data on the port that has been initialized. Any data that is sent to a port that has not been initialized will not be transmitted.

Data Filter

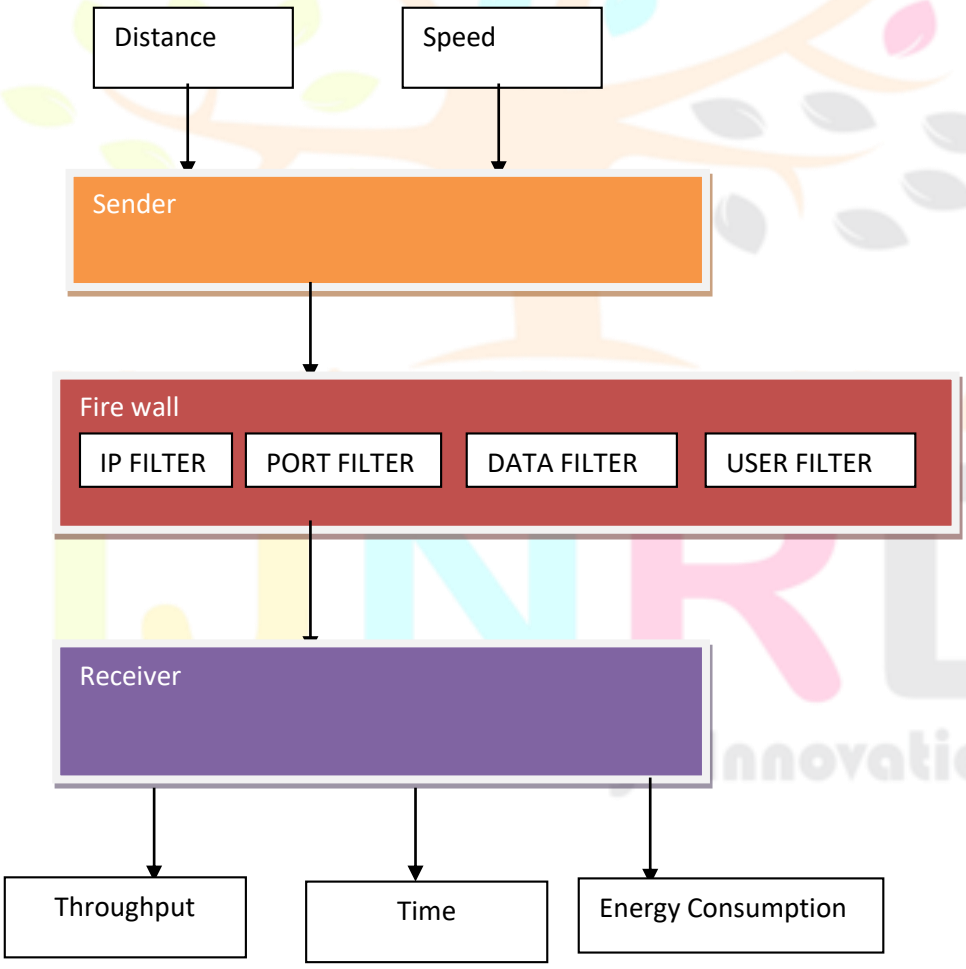
A data filter will restrict data only if it has a particular format, size, and author. These files could be malicious or could be an attempt at some kind of attack. As a result, the work that has been proposed is looking into data filter mechanisms to restrict the transmission of unauthentic data items.

User Filter

This category of filter is able to restrict users who do not have authentic credentials. The user filter-based firewall places restrictions on the restricted user who has limited privileges. It is forbidden for users who have not been authenticated to send or receive packets.

Proposed work

In proposed research compressed data has been send from sender to receiver and IP filter has been used to restrict unauthentic data transmission. Firewall applied in proposed mechanism is providing multilayer security. Data security has been provided by encryption whereas session security allows user to establish session during data transmission. IP filter restrict access of unauthentic IP addresses. User defined port number is allowing user to make use of customized protocol for the multilayer firewall security.



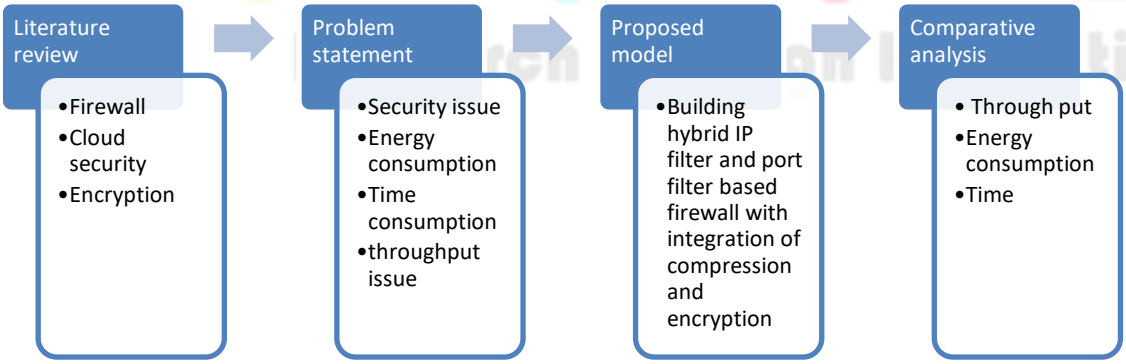
Proposed Model

Present research is considering user filter to restrict authentic user by creating session. Research is also restricting non authentic IP addresses. Only user defined port are considered to make port based filtering. Unauthentic data is restricted

by making use of data filter. The work that is being presented has the ability to compress huge packets and enhance data security by making use of a proposed encryption technique. The study that is being recommended is centred on the encrypting of data in a number of different methods as well as the compressing of data in a variety of various procedures. Both of these are considered to be important aspects of protecting sensitive information. Before delivering the information to the client, the server would first encrypt the data and then compress it. This was done to guarantee that the materials that were being sent were secure. The information obtained from the surveillance system is now labelled with an X classification. The material is then subjected to compression and then burned, which results in the formation of a CX. After that, a technique of encryption is included into the process. After the data has been encrypted, it is then sent to the customer who will ultimately be in possession of it. In order to obtain the information that was initially intended for educational purposes, the data is decompressed here after having been encrypted before. The algorithm to explain the working is explained as follows:

Step 1. Get the data from agriculture area and set content as X
Step 2. Apply compression mechanism on X and get CX
Step 3. Apply xor based encryption mechanism over CX and get ECX
Step 4 Apply user defined port and initiate session at receiver end
Step 5 if session is initiated on receiver end and IP is valid and sender port and receiver port is same
Transfer encrypted data to receiver end
Apply decryption mechanism over ECX and get CX
Apply decompression mechanism over CX and get X
Step 6. Otherwise no operation
Step 7. Stop

In this proposed work, research is considering distance and speed factor over time, throughput, and energy consumption. In the research that has been proposed, data has been sent from sender to receiver in a compressed format, and an IP filter has been utilized to restrict the transmission of data that is not authentic. The application of a firewall in the proposed mechanism provides security on multiple layers. Encryption has been used to ensure the safety of the data, while session security enables users to set up a session even while data is being transmitted. IP filters prevent access for IP addresses that have not been verified. The user is able to make use of a customized protocol thanks to the user-defined port number, which is part of the multilayer firewall security.



Research methodology

Tools and technology used in proposed work

Hardware that is required for the research work:

1. Processor: X86 compatible faster processor with 1 Giga Hertz or Faster
2. Random Access Memory with one Gigabyte or extra.
3. Hard Disk with twenty Gigabyte or extra.
4. Monitor: - Virtual Graphics Adapter
5. Keyboard with 104 keys.
6. Mouse with two or three Button.

Software those are required for the research work:

1. Window Operating System.
2. MATLAB simulation tool.

Comparative analysis of proposed mechanism parameter to conventional parameters

Parameter	**Encrypted data**	**Non-Encrypted data**	**Compressed data**	**Proposed mechanism**
Data transmission speed	20	25	30	35
Time	(sin (B)*B*log2 (1+S/N))/20	(sin (B)*B*log2 (1+S/N))/25	(sin (B)*B*log2 (1+S/N))/30	(sin (B)*B*log2 (1+S/N))/35
Throughput	**1/ (** (sin (B)*B*log2 (1+S/N))/20)	**1/ (** (sin (B)*B*log2 (1+S/N))/25**)**	**1/ (** (sin (B)*B*log2 (1+S/N))/30**)**	**1/ (** (sin (B)*B*log2 (1+S/N))/35**)**
Energy consumption factor	**4**	**3**	**2**	**1**
Energy consumption	1/ (2*sqrt (x.^ (2)/9)/4)	1/ (2*sqrt (x.^ (2)/9)/3)	1/ (2*sqrt (x.^ (2)/9)/2)	1/ (2*sqrt (x.^ (2)/9)/1)

Data transmission simulation with encryption, user-defined ports, and a firewall based on compressed data

In a simulation, the random port number is obtained from the sender after the default port has been initialized. The simulation results below display the sender's randomly assigned port. The user on the receiving end would then need to enter the path to the file containing the received data and the token needed to decode it.

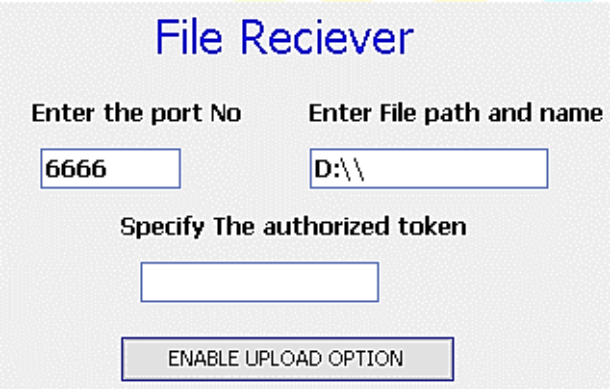


Fig.1 Simulation of receiver node

The same holds true on the sender's end, where the sender specifies both the filename and token to be used in the encoding process. The destination IP address is designated as the location for data transmission. The

following diagram depicts how the data would be sent using a randomized port number greater than 1023.

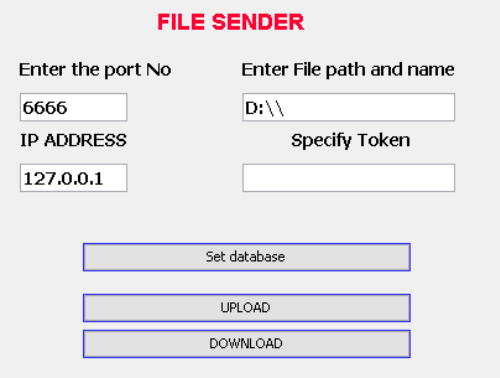


Fig. 2 Simulation of sender node

There remain four cases during data transmission

1.Normal data transmission

In this case, file is transferred directly from sender to receiver in plain format. This data is neither encrypted nor compressed.

2.Data transmission after encryption using conventional mechanism

In this case, file is transferred from sender to receiver in encrypted format. This data is not compressed.

3.Data transmission after compression and encryption using conventional mechanism

In this case, file is transferred from sender to receiver in encrypted format after data compression. Here is encryption is made using conventional RSA mechanism

4.Data transmission after compression and encryption using Proposed mechanism

In this case, file is transferred from sender to receiver in encrypted format after data compression but encryption is made using proposed encryption mechanism.

Comparison of data size, time consumption, throughput

File size is obtained from file properties that are shown in figure 5.3, 5.4, 5.5, 5.6. Considering file size, time consumption factor and energy consumption factor is derived

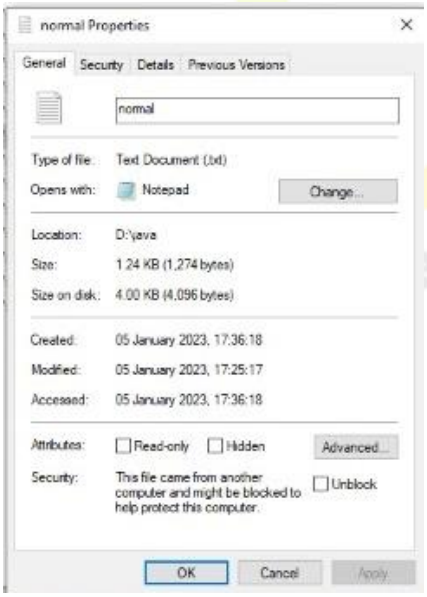


Fig 3 File size in case of Normal data

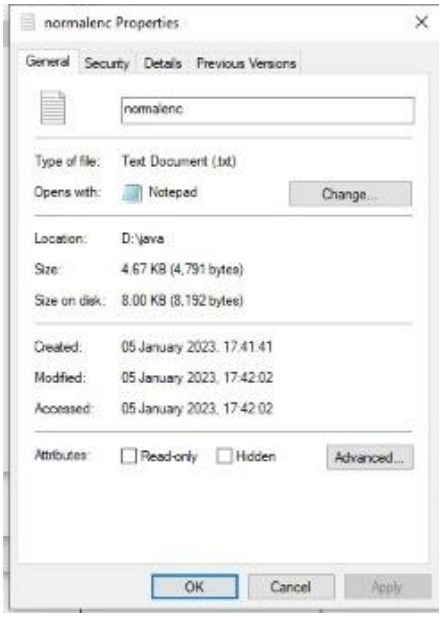


Fig 4 File size in case of conventionally encrypted data

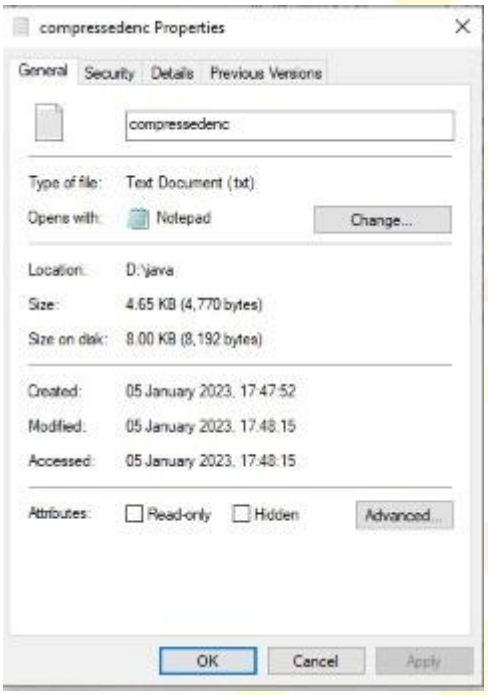


Fig 5 File size in case of conventional encryption based compressed data

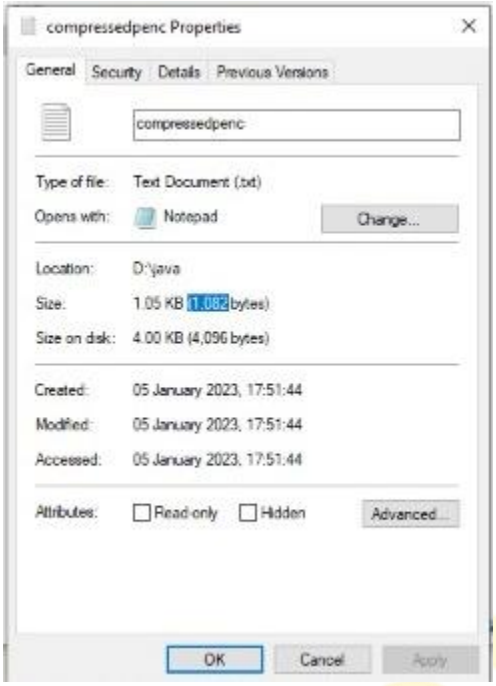


Fig 6 File size in proposed encryption with compression

Table 1 is presenting Comparison of all cases considering file size, time consumption, energy and throughput factor

Table 1 Comparison chart

	Normal :	**Encrypted :**	**Conventional compressed and Encrypted:**	**Proposed Compressed and encrypted**
File size(in bytes)	1,274 Bytes	4,791 Bytes	4,770 Bytes	1,082 Bytes
Time consumption (factor) (considering 1bytes per second)	1274/1024= 1.244141	4791/1024= 4.678710938	4,770/1024= 4.658203125	1082/1024 = 1.056640625
Energy (factor)	1274/1082 = 1.17744916820702	4,791/1082= 4.427911275	4,770/1082= 4.408502773	1,082/1082=1
Here x is distance				
Energy consumption	1/(2*sqrt(x.^(2)/9)/ 1.17744916820702)	1/(2*sqrt(x.^(2)/9)/ 4.427911275)	1/(2*sqrt(x.^(2)/9)/ 4.408502773)	1/(2*sqrt(x.^(2)/9)/1)
Throughput	(sin(B)*B*log2(1+x/N)) /1.244141	(sin(B)*B*log2(1+x/N)) /4.678710938	(sin(B)*B*log2(1+x/N)) /4.658203125	(sin(B)*B*log2(1+x/N)) /1.056640625

Time	1/(sin(B)*B*log2(1+x/N)) /1.244141	1/(sin(B)*B*log2(1+x/N)) /4.678710938	1/(sin(B)*B*log2(1+x/N)) /4.658203125	1/(sin(B)*B*log2(1+x/N)) /1.056640625
Here s is speed from x is distance that is divided by time factor				
Speed factor (s)	x/1.244141	x/4.678710938	x/4.658203125	x/1.056640625
Energy consumption	1/(2*sqrt(s.^(2)/9)/ 1.17744916820702)	1/(2*sqrt(s.^(2)/9)/ 4.427911275)	1/(2*sqrt(s.^(2)/9)/ 4.408502773)	1/(2*sqrt(s.^(2)/9)/1)
Throughput	(sin(B)*B*log2(1+s/N)) /1.244141	(sin(B)*B*log2(1+s/N)) /4.678710938	(sin(B)*B*log2(1+s/N)) /4.658203125	(sin(B)*B*log2(1+s/N)) /1.056640625
Time	1/(sin(B)*B*log2(1+s/N)) /1.244141	1/(sin(B)*B*log2(1+s/N)) /4.678710938	1/(sin(B)*B*log2(1+s/N)) /4.658203125	1/(sin(B)*B*log2(1+s/N)) /1.056640625

Simulation

Considering table 1 simulation and graphical presentation is shown in this section

Table 2 is considering Comparative analysis of file size

Table 2 File size comparison

Normal :	**Encrypted :**	**Conventional compressed and Encrypted:**	**Proposed Compressed and encrypted:**
1,274	4,791	4,770	1,082

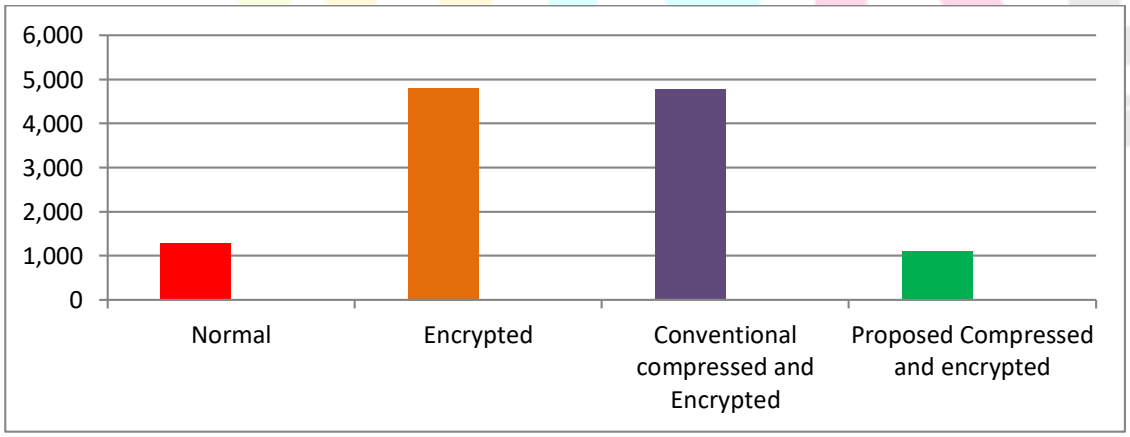


Fig 7 Comparison of file size

Considering energy efficiency equation shown in table 1, following table has been generated to simulate energy consumption in different cases for distance ranging 1 to 40

Table 5.3 Comparative analysis of energy efficiency

Distance	Normal	Encrypted	Conventional compressed and Encrypted	Proposed Compressed and encrypted
1	0.5662	0.1506	0.1512	0.6667
2	1.1324	0.3011	0.3024	1.3333
3	1.6986	0.4517	0.4537	2
4	2.2648	0.6022	0.6049	2.6667
5	2.831	0.7528	0.7561	3.3333
6	3.3972	0.9034	0.9073	4
7	3.9634	1.0539	1.0586	4.6667
8	4.5296	1.2045	1.2098	5.3333
9	5.0958	1.355	1.361	6
10	5.662	1.5056	1.5122	6.6667
11	6.2282	1.6562	1.6635	7.3333
12	6.7943	1.8067	1.8147	8
13	7.3605	1.9573	1.9659	8.6667
14	7.9267	2.1078	2.1171	9.3333
15	8.4929	2.2584	2.2683	10
16	9.0591	2.409	2.4196	10.6667
17	9.6253	2.5595	2.5708	11.3333
18	10.1915	2.7101	2.722	12
19	10.7577	2.8606	2.8732	12.6667
20	11.3239	3.0112	3.0245	13.3333
21	11.8901	3.1618	3.1757	14
22	12.4563	3.3123	3.3269	14.6667
23	13.0225	3.4629	3.4781	15.3333
24	13.5887	3.6134	3.6294	16
25	14.1549	3.764	3.7806	16.6667
26	14.7211	3.9146	3.9318	17.3333
27	15.2873	4.0651	4.083	18
28	15.8535	4.2157	4.2342	18.6667
29	16.4197	4.3662	4.3855	19.3333
30	16.9859	4.5168	4.5367	20
31	17.5521	4.6674	4.6879	20.6667
32	18.1183	4.8179	4.8391	21.3333
33	18.6845	4.9685	4.9904	22
34	19.2507	5.119	5.1416	22.6667
35	19.8168	5.2696	5.2928	23.3333
36	20.383	5.4202	5.444	24
37	20.9492	5.5707	5.5952	24.6667
38	21.5154	5.7213	5.7465	25.3333
39	22.0816	5.8718	5.8977	26
40	22.6478	6.0224	6.0489	26.6667

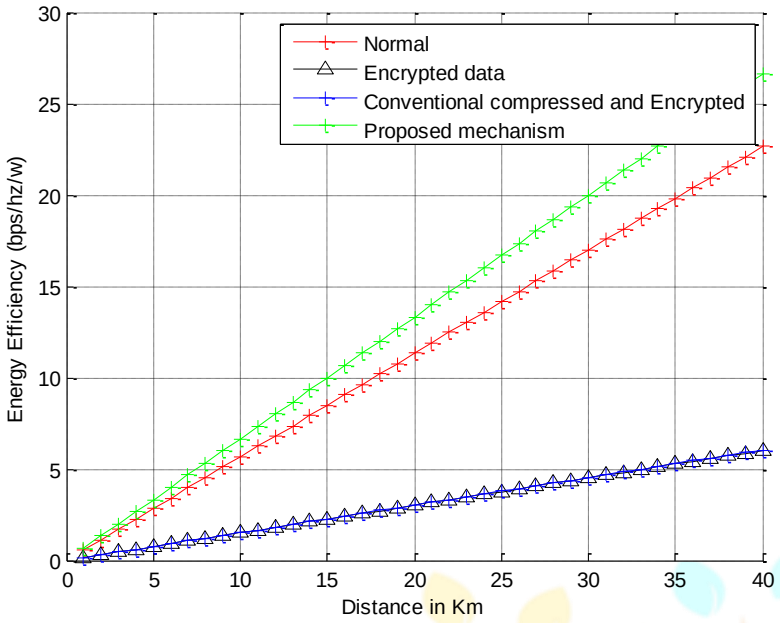


Fig 8 Comparison of energy efficiency considering distance

Considering time consumption equation shown in table 1, following table has been generated to simulate time consumption in different cases for distance ranging 1 to 40

Table 4 Comparison of time consumption

Distance	Normal	Encrypted	Conventional compressed and Encrypted	Proposed Compressed and encrypted
1	1.1718	4.4066	4.3873	0.9952
2	0.593	2.2302	2.2204	0.5037
3	0.4001	1.5046	1.498	0.3398
4	0.3036	1.1416	1.1366	0.2578
5	0.2457	0.9238	0.9198	0.2086
6	0.207	0.7785	0.7751	0.1758
7	0.1794	0.6747	0.6718	0.1524
8	0.1587	0.5968	0.5942	0.1348
9	0.1426	0.5362	0.5338	0.1211
10	0.1297	0.4876	0.4855	0.1101
11	0.1191	0.4479	0.4459	0.1011
12	0.1103	0.4147	0.4129	0.0937
13	0.1028	0.3867	0.385	0.0873
14	0.0964	0.3626	0.361	0.0819
15	0.0909	0.3417	0.3402	0.0772
16	0.086	0.3234	0.322	0.073
17	0.0817	0.3072	0.3059	0.0694
18	0.0779	0.2928	0.2916	0.0661
19	0.0744	0.28	0.2787	0.0632
20	0.0714	0.2684	0.2672	0.0606
21	0.0686	0.2578	0.2567	0.0582
22	0.066	0.2483	0.2472	0.0561
23	0.0637	0.2395	0.2385	0.0541
24	0.0616	0.2315	0.2305	0.0523
25	0.0596	0.2241	0.2231	0.0506
26	0.0578	0.2173	0.2163	0.0491
27	0.0561	0.2109	0.21	0.0476
28	0.0545	0.2051	0.2042	0.0463
29	0.0531	0.1996	0.1987	0.0451
30	0.0517	0.1944	0.1936	0.0439

31	0.0504	0.1896	0.1888	0.0428
32	0.0492	0.1851	0.1843	0.0418
33	0.0481	0.1809	0.1801	0.0408
34	0.047	0.1769	0.1761	0.0399
35	0.046	0.1731	0.1723	0.0391
36	0.0451	0.1695	0.1688	0.0383
37	0.0442	0.1661	0.1654	0.0375
38	0.0433	0.1629	0.1622	0.0368
39	0.0425	0.1599	0.1592	0.0361
40	0.0417	0.157	0.1563	0.0355

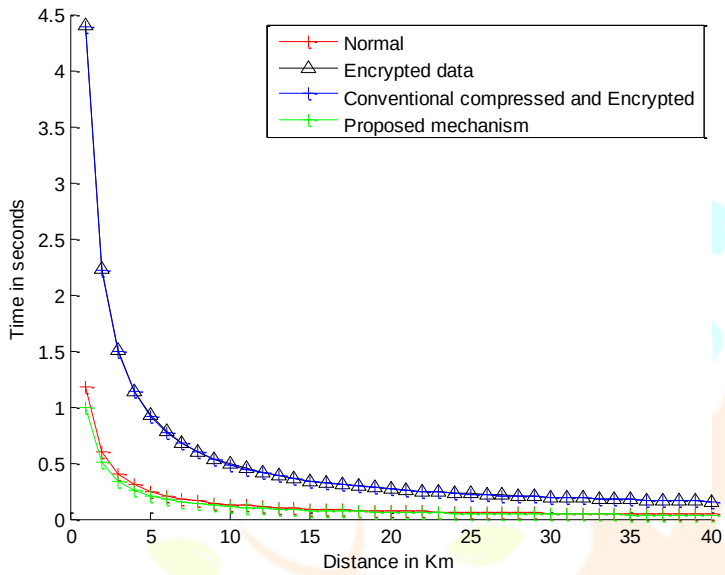


Fig 9 Time consumption comparison considering distance

Table 5 Comparison of Throughput

Distance	**Normal**	**Encrypted**	**Conventional compressed and Encrypted**	**Proposed Compressed and encrypted**
1	0.8534	0.2269	0.2279	1.0048
2	1.6862	0.4484	0.4504	1.9855
3	2.4995	0.6646	0.6676	2.943
4	3.294	0.8759	0.8798	3.8785
5	4.0707	1.0825	1.0872	4.7931
6	4.8303	1.2845	1.2901	5.6875
7	5.5736	1.4821	1.4886	6.5626
8	6.3012	1.6756	1.683	7.4194
9	7.0139	1.8651	1.8733	8.2585
10	7.7121	2.0508	2.0598	9.0806
11	8.3965	2.2328	2.2426	9.8864
12	9.0676	2.4112	2.4218	10.6766
13	9.7259	2.5863	2.5977	11.4518
14	10.3719	2.7581	2.7702	12.2124
15	11.0061	2.9267	2.9396	12.9591
16	11.6288	3.0923	3.1059	13.6924
17	12.2406	3.255	3.2693	14.4126
18	12.8416	3.4148	3.4298	15.1204
19	13.4324	3.5719	3.5876	15.816
20	14.0133	3.7264	3.7428	16.5

21	14.5846	3.8783	3.8953	17.1726
22	15.1466	4.0277	4.0454	17.8343
23	15.6995	4.1748	4.1931	18.4854
24	16.2438	4.3195	4.3385	19.1263
25	16.7797	4.462	4.4816	19.7572
26	17.3073	4.6023	4.6225	20.3785
27	17.8271	4.7405	4.7614	20.9905
28	18.3391	4.8766	4.8981	21.5933
29	18.8436	5.0108	5.0329	22.1874
30	19.3409	5.143	5.1657	22.773
31	19.8312	5.2734	5.2966	23.3502
32	20.3145	5.4019	5.4257	23.9193
33	20.7912	5.5287	5.5531	24.4806
34	21.2615	5.6538	5.6786	25.0343
35	21.7254	5.7771	5.8025	25.5805
36	22.1832	5.8988	5.9248	26.1195
37	22.6349	6.019	6.0455	26.6515
38	23.0809	6.1376	6.1646	27.1766
39	23.5212	6.2546	6.2822	27.695
40	23.9559	6.3702	6.3983	28.2069

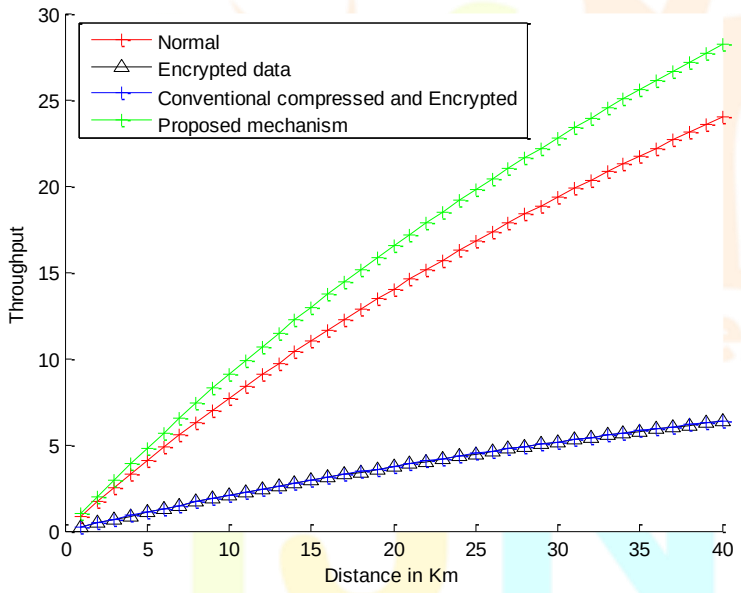


Fig 10 Comparison of throughput considering distance

Comparison of energy efficiency considering speed

Speed	Normal	Encrypted	Conventional compressed and Encrypted	Proposed Compressed and encrypted
1	0.4551	0.0322	0.0325	0.6309
2	0.9102	0.0644	0.0649	1.2619
3	1.3653	0.0965	0.0974	1.8928
4	1.8204	0.1287	0.1299	2.5237
5	2.2754	0.1609	0.1623	3.1547
6	2.7305	0.1931	0.1948	3.7856

7	3.1856	0.2253	0.2272	4.4165
8	3.6407	0.2574	0.2597	5.0474
9	4.0958	0.2896	0.2922	5.6784
10	4.5509	0.3218	0.3246	6.3093
11	5.006	0.354	0.3571	6.9402
12	5.4611	0.3862	0.3896	7.5712
13	5.9162	0.4183	0.422	8.2021
14	6.3713	0.4505	0.4545	8.833
15	6.8263	0.4827	0.487	9.464
16	7.2814	0.5149	0.5194	10.0949
17	7.7365	0.5471	0.5519	10.7258
18	8.1916	0.5792	0.5843	11.3567
19	8.6467	0.6114	0.6168	11.9877
20	9.1018	0.6436	0.6493	12.6186

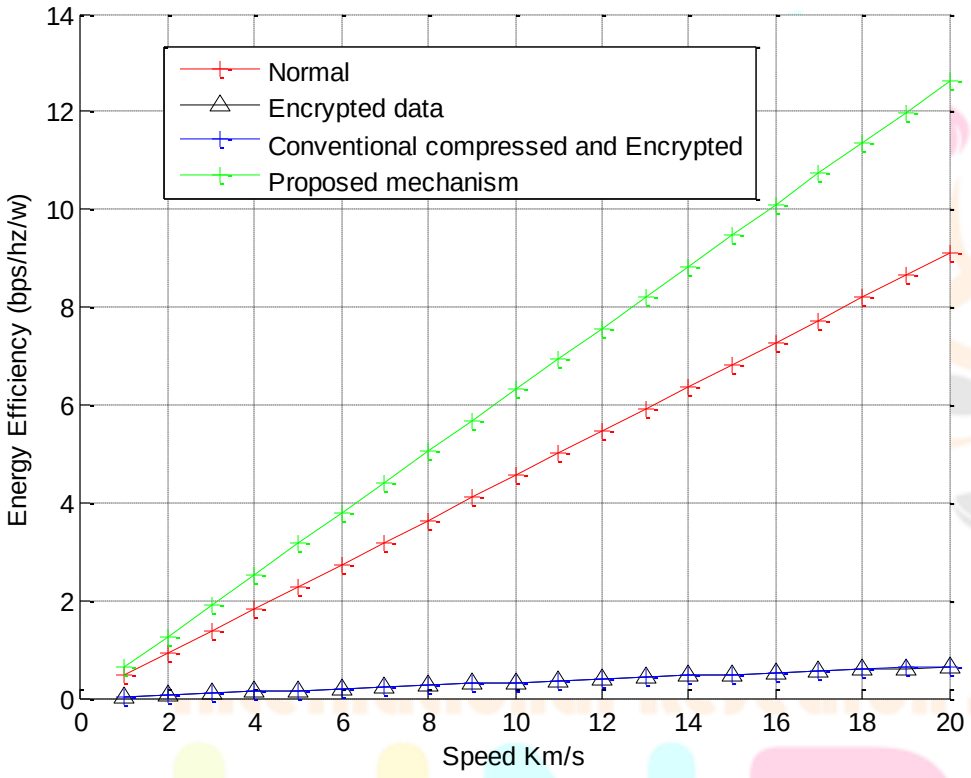


Fig 11 Energy comparison considering speed factor

Comparison of energy efficiency considering speed

Speed	**Normal**	**Encrypted**	**Conventional compressed and Encrypted**	**Proposed Compressed and encrypted**
1	0.7261	0.049	0.0494	0.9516
2	1.4373	0.0977	0.0986	1.8815
3	2.1342	0.1462	0.1474	2.7905
4	2.8172	0.1944	0.1961	3.6798
5	3.4871	0.2423	0.2444	4.55
6	4.1442	0.29	0.2926	5.4019
7	4.789	0.3375	0.3404	6.2364
8	5.422	0.3847	0.3881	7.0542
9	6.0437	0.4317	0.4354	7.8558
10	6.6543	0.4784	0.4826	8.642
11	7.2544	0.5249	0.5295	9.4132
12	7.8442	0.5712	0.5761	10.1701

13	8.4241	0.6172	0.6226	10.9132
14	8.9945	0.663	0.6687	11.6429
15	9.5556	0.7086	0.7147	12.3598
16	10.1077	0.7539	0.7604	13.0643
17	10.6511	0.7991	0.806	13.7568
18	11.1862	0.844	0.8512	14.4377
19	11.713	0.8887	0.8963	15.1074
20	12.232	0.9331	0.9412	15.7663

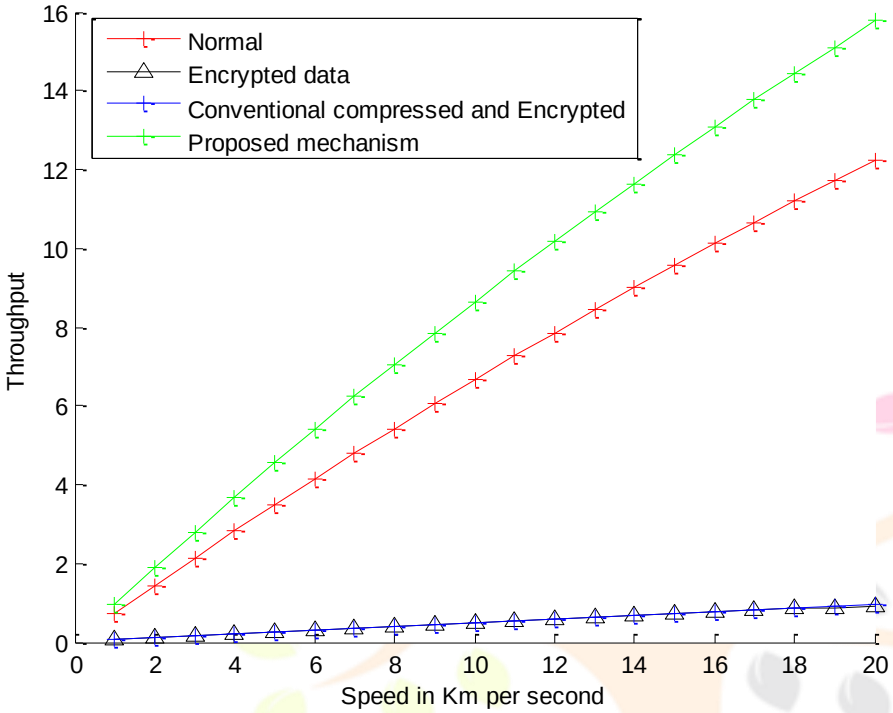


Fig 12 Throughput considering speed factor

Comparison of time consumption considering speed

Speed	Normal	Encrypted	Conventional compressed and Encrypted	Proposed Compressed and encrypted
1	1.3772	20.418	20.2396	1.0509
2	0.6957	10.2361	10.1468	0.5315
3	0.4686	6.8421	6.7825	0.3584
4	0.355	5.1451	5.1004	0.2718
5	0.2868	4.1269	4.091	0.2198
6	0.2413	3.4481	3.4181	0.1851
7	0.2088	2.9632	2.9375	0.1603
8	0.1844	2.5995	2.577	0.1418
9	0.1655	2.3166	2.2966	0.1273
10	0.1503	2.0903	2.0722	0.1157
11	0.1378	1.9051	1.8887	0.1062
12	0.1275	1.7508	1.7357	0.0983
13	0.1187	1.6202	1.6063	0.0916
14	0.1112	1.5083	1.4953	0.0859
15	0.1047	1.4113	1.3992	0.0809
16	0.0989	1.3264	1.315	0.0765
17	0.0939	1.2515	1.2408	0.0727
18	0.0894	1.1849	1.1748	0.0693

19	0.0854	1.1253	1.1157	0.0662
20	0.0818	1.0717	1.0625	0.0634

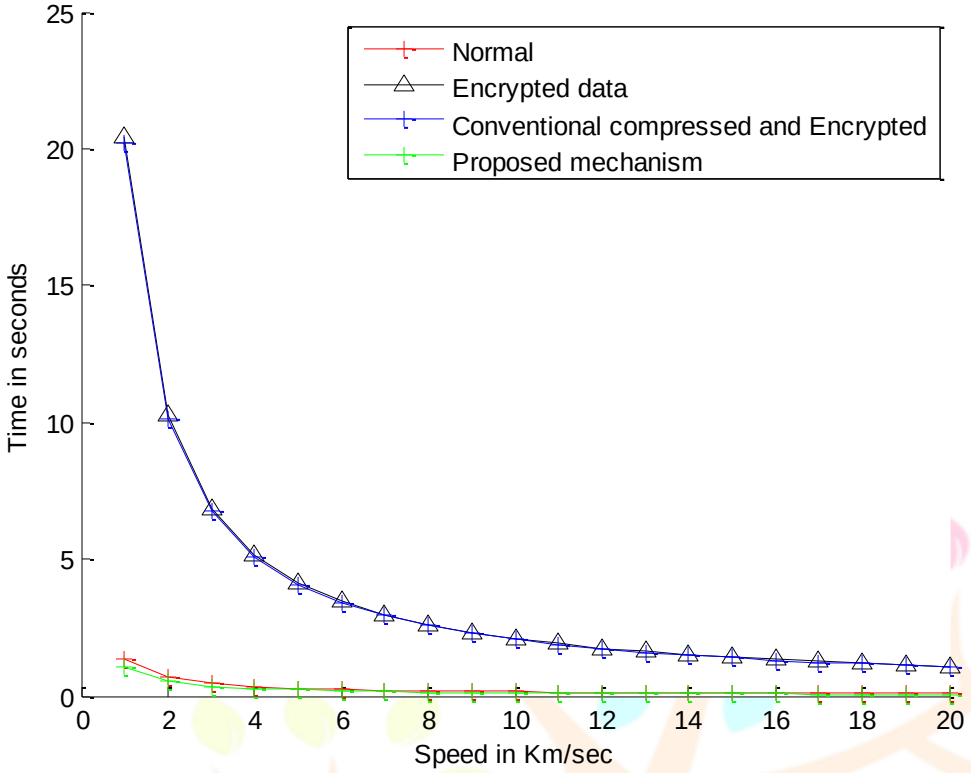


Fig 13 Time considering speed factor

Summary

It has been seen that factors such as speed and distance have a major influence on the amount of time, energy used, and throughput. According to the findings of the simulation, the suggested firewall has a higher throughput than the traditional encryption-based firewall mechanism. This is because the proposed firewall takes into account compression and encryption in addition to the IP and port filtering method. The work that is being proposed also results in a reduction in the amount of time and energy required for data transmission. Additionally, it has been noticed that the suggested firewall decreases the likelihood of an attack happening while it is in use.

References:

A. D. Brucker (2015), L. Br¨ugger, and B. Wolff. Formal firewall conformance testing: An application of test and proof techniques. Softw. Test. Verif. Reliab., Vol 25 (1), pg. 34–71

A. Hari, S. Suri, and G. Parulkar (2000). Detecting and Resolving Packet Filter Conflicts. 19th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM, Vol 3, pg. 1203–1212

A. Launay (2016). High Level Firewall Language. https://www.cusae.com/ hlfl/.

A. Liu and M. Gouda (2004). Diverse Firewall Design. 34th IEEE International Conference on Dependable Systems and Networks (DSN), Florence, Italy, pg. 595–604

A. Liu, M. Gouda (2004), H. Ma, and A. Hgu. Firewall Queries. 8th International Conference, On Principles of

Distributed Systems (OPODIS), Grenoble, France, pg. 197–212

A. Mayer, A. Wool, and E. Ziskind (2000). Fang: A Firewall Analysis Engine. 21st IEEE Symposium on Security and Privacy, Oakland, CA, USA, pg. 44-52

A. Mayer, A (2006). Wool, and E. Ziskind. Offline Firewall Analysis. International Journal of Information Security, Vol 5 (3), pg. 125–144

A.Nawaz,.et al. (2006) Game theory and intrusion detection systems. pg. 152-159

Ahmed Jamal, A., et al., (2021). A review on security analysis of cyber physical systems using machine learning. Mater, pg. 302-312

Akanksha Chaudhary & Dr.Shrddha Sagar (2016), Analytical Study of Packet Filtering Firewall, pg. 256-260

Al-Ghamdi, M.I., (2021). Effects of knowledge of cyber security on prevention of attacks. Mater. pg. 126-132

B. Aziz, S.N. Foley, J. Herbert, and G. Swart (2009). Configuring storage-area networks using mandatory security. Journal of Computer Security, Vol 17 (2), pg. 191– 210.

B. Dempster and J. Eaton-Lee (2006). Configuring IPCop Firewalls: Closing Borders with Open Source: How to set up, configure, and manage your Linux firewall, web proxy, DHCP, DNS, time server, and VPN with this powerful Open Source solution. pg. 96-102

Bavithra.G.R, Mahalakshmi.V, R.Suganya (2018), A Review on Firewall and its Attacks, Vol. 7, Issue 1, pg. 48-52

Chirag Sheth& Rajesh Thakker (2011), Performance Evaluation and Comparative Analysis of Network Firewalls, pg. 162-168

Damodharan, Prabhat Kumar Srivastava (2018). A Review Paper on Computer Firewall. International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 2, pg. 76-88

Dr. A R. PonPeriyasamy (2017), Security Issues of Firewall, Volume-7, Issue-7, pg. 32-44

Dr. Ajitsingh, Madhu Pahal, Neeraj Goyat (2013), A Review Paper On Firewall, Vol. 1 Issue II, pg. 106-112

Dr. Pranav Patil &Suyog Vijay Kulkarni (2019), Protect of Security: Firewalls, Vol.7 Issue. 10, October- 2019, pg. 17-21

E. Al-Shaer and H. Hamed (2003). Firewall Policy Advisor for Anomaly Discovery and Rule Editing. 8th IFIP/IEEE International Symposium on Integrated Network Management, Colorado Springs, USA, pg. 222-228

E. Al-Shaer, H. Hamed, R. Boutaba, and M. Hasan (2005). Conflict Classification and Analysis of Distributed Firewall Policies. IEEE Journal on Selected Areas in Communications, Issue: 10, Volume: 23, pg. 2069 - 2084

Er. Shikha Pandit, Er. Pritam Kumar, Er. Deepak Malik (2014), Fire-Router: A new secure inter-networking device, Vol. 3, Issue. 6, pg.279 – 285

F. Cuppens, N. Cuppens-Boulahia, and J. Garc´ıa-Alfaro (2005). Detection and Removal of Firewall Misconfiguration. IASTED International Conference on Communication, Network and Information Security (CNIS), pg. 56-62

F. Cuppens, N. Cuppens-Boulahia, J. Garc´ıa-Alfaro, T. Moataz, and X. Rimasson (2012). Handling stateful firewall anomalies. In Information Security and Privacy Research - 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings, pg. 174–186.

He, X. (2021). Research on Computer Network Security Based on Firewall Technology. In Journal of Physics: Conference Series (Vol. 1744, Issue 4, pg. 42-52. IOP Publishing. https://doi.org/10.1088/1742-6596/1744/4/042037

I. Kashefi, Maryam Kassiri, Ali Shahidinejad (2013). A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities. pg. 218-224

J. Garc´ıa-Alfaro, F. Cuppens, N. Cuppens-Boulahia, S. Mart´ınez Perez, and J. Cabot (2013). Management of stateful firewall misconfiguration. Computers & Security, Vol 39, pg. 64–85

J.J. Barbish. IPFW (2016) - FreeBSD firewall. https://www.cisco.com/c/ en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/ scfacls.html. [Online; accessed August-2016].

K. Golnabi, R. Min, L. Khan, and E. Al-Shaer (2006). Analysis of Firewall Policy Rule Using Data Mining Techniques. 10th IEEE/IFIP Network Operations and Management Symposium (NOMS), Vancouver, Canada, pg. 256-262

K. Scarfone and P. Hoffman (2009). Guidelines on Firewalls and Firewall Policy: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-41, Revision 1, pg. 19-23

Khaled Salah, Khalid Elbadawi, Raouf Boutaba (2012), Performance Modelling and Analysis of Network Firewalls, Volume: 9 , Issue: 1, pg. 71-78

Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. Computers & Security, Vol 25 (7), pg. 522-538.

Konikiewicz, Wojciech &Markowski, Marcin. (2017). Analysis of Performance and Efficiency of Hardware and Software Firewalls. Journal of Applied Computer Science Methods. Vol. 9, No. 1, pg. 49-56.

L Dong et al.[2012]. Network Security and Firewall Technology [C]. pg. 232-238

L. Buttyan, G. P´ek, and T. Vinh Thong (2009). Consistency verification of stateful firewalls is not harder than the stateless case. Infocommunications Journal, Vol 64 (1), pg. 2–8.

L. Gheorghe (2006). Designing and Implementing Linux Firewalls with QoS using netfilter, iproute, NAT and l7-filter. PACKT Publishing, pg. 36-42.

M Murphy, et al. (2016) Ford's connected car cloud offering will be powered by Microsoft Azure. pg. 42-48. DOI 10.1186/s13635-016-0042-3.