ENCRYPTED IP AND RANDOM KEY BASED NETWORK COMMUNICATION SYSTEM

[1] Monica Pancholi,[2]Mrs. Shalini

[1] MTech. Scholar, [2] Assistant Professor
[1]Name of Department of 1st Author,
[1,2] Department of Computer Science& Engineering, Jaipur Institute of Technology Group of Institutions ,,Jaipur, Rajasthan ,India

Abstract: Transferring the data in the secure way is very essential for the network communication system..The proposed work deals with the encrypting of the IP address as well as encrypting of the message with the HASH based algorithm SHA used for the verification purpose. The key formed comprises of the SHA Hash makes it stronger for hackers to crack.

***Index Terms* - Data Network Security, SHA verification.**

I. INTRODUCTION

Network security is a general term that portrays that the arrangements and systems actualized by a network manager to stay away from and monitor unapproved get to, misuse, alteration, or forswearing of the network and network resources. This implies that a very much executed network security squares infections, malware, programmers, and so on from getting to or changing secure information. [1]

The primary layer of network security is upheld through a username/secret phrase system, which just enables access to validated clients with redid benefits. At the point when a client is confirmed and allowed explicit framework get to, the arranged firewall upholds network strategies, that is, open client services. However, firewalls don't generally identify and stop infections or unsafe malware, which may prompt data misfortune. An enemy of infection programming or an interruption counteractive action framework (IPS) is actualized to keep the infection or potentially unsafe malware from entering the network.[1]

Network security is now and again mistaken for information security, which has an alternate extension and identifies with data integrity all things considered, print or electronic. Network security is a specific field in PC networking that includes verifying a PC network foundation. Network security is normally taken care of by a network overseer or framework director who actualizes the security strategy, network programming and equipment expected to secure a network and the assets got to through the network from unapproved get to and furthermore guarantee that representatives have sufficient access to the network and assets to work. [2]

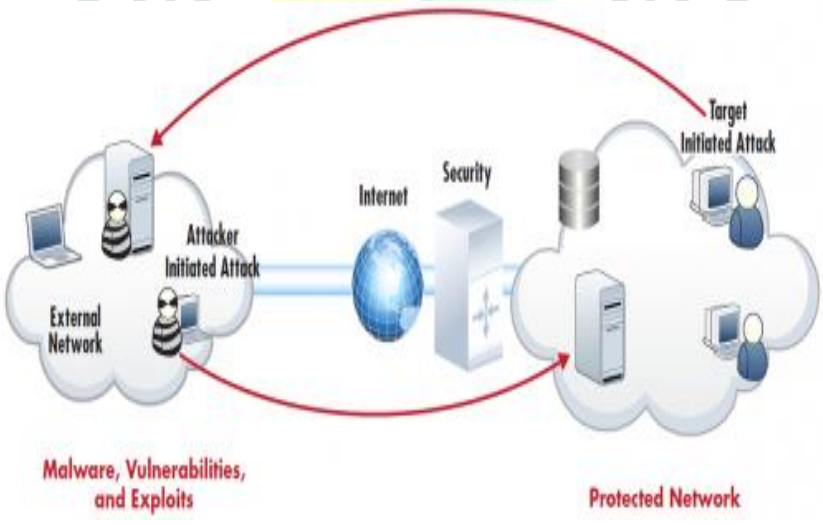


Fig 1. Computer Security Concept

A network security framework ordinarily depends on layers of insurance and comprises of different segments including networking observing and security programming notwithstanding equipment and apparatuses. All parts cooperate to expand the general security of the PC network. [2].

II. IP ADDRESSES

IP address goes about as an identifier for a particular machine on a specific network. The IP address is likewise called IP number and web address. IP address determines the specialized configuration of the tending to and packets conspire. Most networks consolidate IP with a TCP (Transmission Control Protocol). It likewise permits building up a virtual association between a goal and a source. IPv4 was the primary adaptation of IP. It was conveyed for creation in the ARPANET in 1983. Today it is most generally utilized IP rendition. It is utilized to distinguish gadgets on a network utilizing a tending to system. [3]

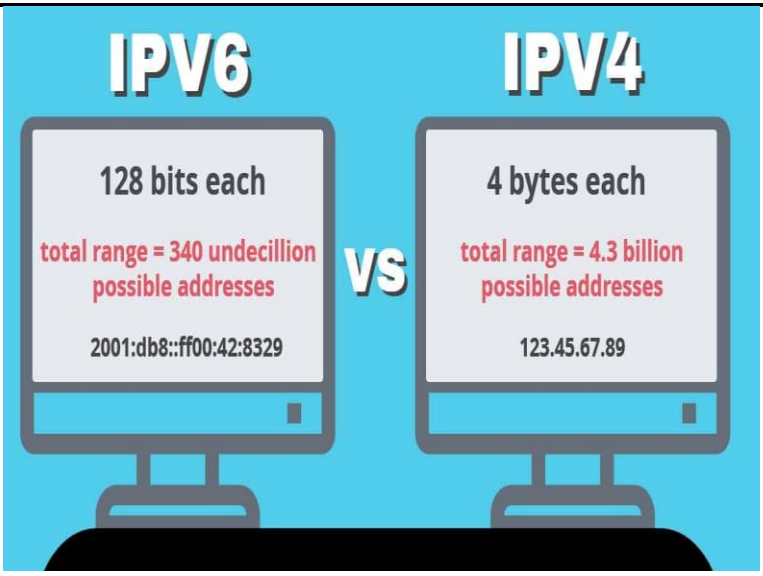
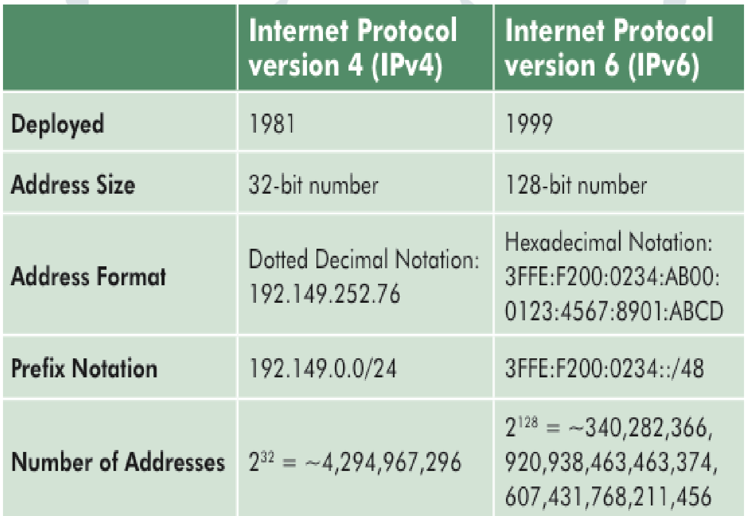

IPV6
IPV4
128 bits each
total range = 340 undecillion possible addresses
2001:db8::ff00:42:8329
VS
4 bytes each
total range = 4.3 billion possible addresses
123.45.67.89

Fig 2. IP4 and IP6 Address

The IPv4 utilizes a 32-bit address conspire permitting to store 2^32 tends to which is in excess of 4 billion locations. Till date, it is viewed as the essential Internet Protocol and conveys 94% of Internet traffic. It is the latest variant of the Internet Protocol. Web Engineer Taskforce started it in mid 1994. The structure and improvement of that suite is presently called IPv6.This new IP address form is being sent to satisfy the requirement for more Internet addresses. It was planned to determine issues which are related with IPv4. With 128-piece address space, it permits 340 undecillion one of a kind location space. IPv6 likewise called IPng (Internet Protocol people to come). [3].



	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

Fig 3. Difference between IPv4 and IPv6

III. Related Work

Shikhi Singh, Rohit Singh, 2017 [4]In current Internet directing structure, the switch doesn't break down or affirm the exactness of the source address passed on in the group, neither has it secured the state information when sending the bundle. Therefore the DDoS ambushes with caricatured IP source address can achieves causing the security issues. In this paper, our point is to shield the attackers from striking some spot outside the IPv6 edge facilitate with fabricated source address in the fine granularity. In this makers have proposed a twofold security figuring, when encode the message just as scramble the key similarly as IP to which the message is to be send. The IP address is splited into the four segments and nearly the key of 4 characters is used in our estimation which is used for scrambling the IP by expanding the estimation of the all of the IP part and the last piece of the IP address is associated with the key in order to also encode the key.

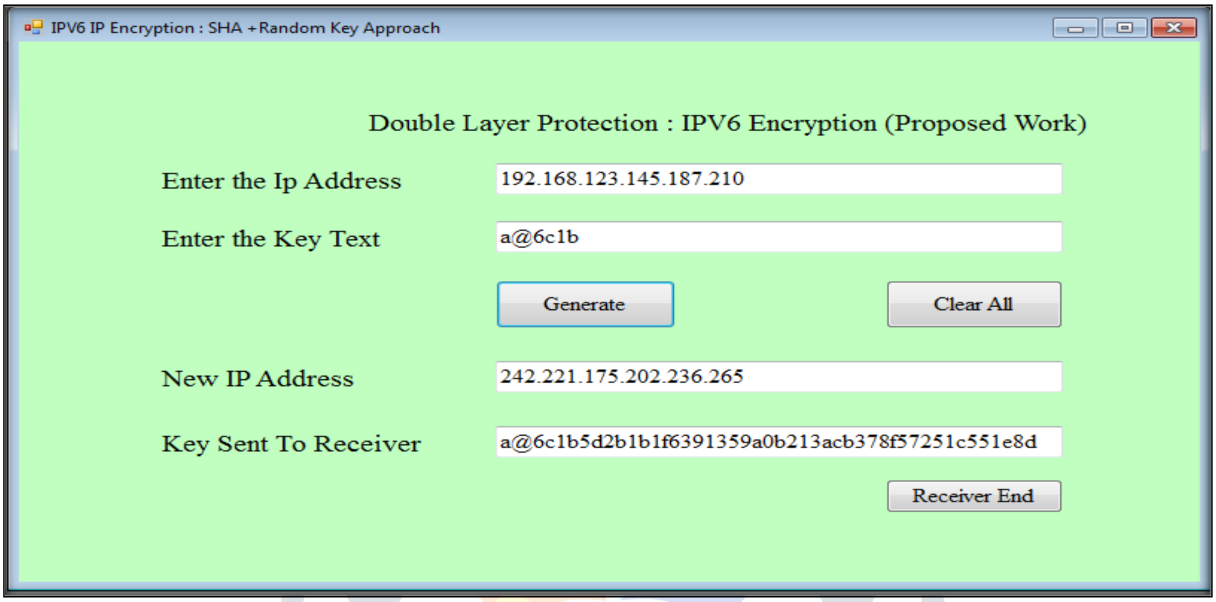
S. Rajashree, et. al ,2018 [5] ,The expansive use of web is causing increasingly advanced attacks using IP criticizing. The security for IoT devices to check IP ridiculing incorporates affirming the source address of got IP packets at the door. This is required to keep an unapproved customer from using IP address as source address and flooding packets to the portal there by using the transmission limit assigned to affirmed customers. This paper proposes an arrangement for IP address errand to splendid IoT contraptions (which confer using TCP/IP) and endorsement of source IP address in the got IP packets from the IoT Device at the Gateway device.

A. Alzahrani and F. Gebali, 2018 [6] Embedded multi-focus structures are executed as structures on-chip that rely upon bundle storeand-forward frameworks on-chip for exchanges. These structures don't use transports or overall clock. Or maybe changes are used to move data between the focuses, and each inside utilizations its own neighborhood clock. This recommends synchronous odd handling. Realizing counts in such structures is particularly supported using dataflow thoughts. In this paper, we propose a technique for completing estimations on dataflow stages. The method can be associated with multi-hung, multi-focus stages or a mix of these stages too. This system relies upon a novel dataflow outline depiction of the count. We associated the proposed theory to get a novel dataflow multi-focus figuring model for the protected hash estimation 3. The resulting gear was completed in field-programmable passage group to check the execution parameters. The major favored viewpoint of this suggestion is ability to logically jumble figuring appraisal to irritate side-channel strikes without refreshing the structure. This has fundamental repercussions for cryptographic applications.

.

IV. Proposed Work

In this paper, we have proposed an answer so as to twofold ensure the entire framework. In the IPv6, the six octet are encoded utilizing the key which is powerfully created utilizing the arbitrary numbers and the ASCII estimation of the each character is registered and included to the octet esteem, after that the SHA is figured for the first IP and linked with the key and after that the scrambled IP and key are sent to the collector. At the beneficiary end, the key characters are isolated from the SHA code and the unscrambling is finished by subtraction of the ASCII esteems and after that the SHA code is again figured and confirmed with the got SHA code to check for the integrity.



IPV6 IP Encryption : SHA +Random Key Approach

Double Layer Protection : IPV6 Encryption (Proposed Work)

Enter the Ip Address: 192.168.123.145.187.210

Enter the Key Text: a@6c1b

New IP Address: 242.221.175.202.236.265

Key Sent To Receiver: a@6c1b5d2b1b1f6391359a0b213acb378f57251c551e8d

Fig 4. Proposed Implementation

Fig. 4 shows the IPV6 proposed work, in this proposed work, the key of 6 characters is taken, produce the SHA Code of Key which is 40 characters string, 6 characters will be chosen from the string and the idea is that the IP address which is isolated by the period is splitted based on the period and after that the ASCII estimations of the four characters comprising the key is determined and added to the six IP parts and thus we get the encoded IP address. Furthermore, for the key, we will separate the last IP part of our genuine IP and connected with the KEY to shape the new EKEY.

V. Result Analysis

The result analysis is done by comparing the strength of the key generated in the base paper work and the proposed work implementation , and tested using the some of the online tools for testing the strength of both the works.
The base work generates the six characters keys e.g. abc41s
The proposed work generates the six random characters key with the SHA of the original IP address.e.g.

ha@1ax698a7ea88c5735a6c2afbc1ab990d3a50cefe9bd2

The results of the comparison with the base and the proposed work are shown in the table 1.

Tools Used	Base Paper Work	Proposed Paper Work
Kaspersky Password Checker	Cracked 3 Hours	More that 1 Year
howsecureismypassword.net	54 milliseconds	232 months
www.my1login.com/resources/password-strength-test/	0.07 seconds	255 days

Table 1 Comparison Analysis Of The Works

VI. Conclusion

The proposed methodology using the possibility of the IP Encryption and Message Encryption utilizing the SHA improved the security and will have extended the weight on the software engineers to part the figure content, resultant in an incredibly secure figure content. And furthermore the sectioned pictures for the secret word age for message sending are additionally utilized.

In the paper, the resultant figure content is attempted over the diverse on the web and disengaged instruments for testing the nature of the figure and the result got are brilliant.

References

[1] J Sagisi, J Tront, R Marchany, "System architectural design of a hardware engine for moving target IPv6 defense ",IEEE,2017

[2] K. Zeitz, M. Cantrell, R. Marchany and J. Tront, "Designing a Micro-moving Target IPv6 Defense for the Internet of Things," IEEE, 2017

[3] W. Sun, C. Gao and J. Sun, "Mobile IPV6 Fast Switching Technology Research," 2016 International Conference on Network and Information Systems for Computers (ICNISC), Wuhan, 2016, pp. 124-127.

[4] Shikhi Singh, RohitSingh , "Double Security algorithm for Network Security",International Journal of Scientific & Engineering Research, Volume 8, Issue 3, March-2017.

[5] S. Rajashree, K. S. Soman and P. G. Shah, "Security with IP Address Assignment and Spoofing for Smart IOT Devices," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, 2018, pp. 1914-1918.

[6] A.Alzahrani and F. Gebali, "Multi-Core Dataflow Design and Implementation of Secure Hash Algorithm-3," in IEEE Access, vol. 6, pp. 6092-6102, 2018.

[7] H. Modares, A. Moravejosharieh, J. Lloret and R. B. Salleh, "A Survey on Proxy Mobile IPv6 Handover," in IEEE Systems Journal, vol. 10, no. 1, pp. 208-217, March 2016..

[8] Tao Zhang and Zhilong Wang, "Research on IPv6 Neighbor Discovery Protocol (NDP) security," 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2016, pp. 2032-2035..

[9] B Chatfield, RJ Haddad,"Moving Target Defense Intrusion Detection System for IPv6 based smart grid advanced metering infrastructure",SoutheastCon, 2017.

[10] Anjali Somwanshi,DevikaKarmalkar,SachiAgrawal,PoonamNanaware,Mrs. GeetanjaliSharma, "Dynamic Grid Based Authentication With Improved Security ",International Journal of Advances in Scientific Research and Engineering (ijasre) ,Vol. 03, Issue 3, April -2017