Secure IP and Data Transmission in Networks

Pooja Yadav[1], Amit Kumar Mishra[2]
[1]M.Tech Scholar, Department of Computer Science and Engineering, Sri Balaji Coleege Engg. & Technology, Jaipur
[3]Assistant Professor, Department of Computer Science and Engineering, Sri Balaji Coleege Engg. & Technology, Jaipur

***Abstract*- In the networks, its utmost important to send the data securely and with integrity or correctness. The proposed aims to improve the security using the encryption of the network IP address and the encryption of the message.**

Index Terms- Encrypted Messages, Encrypted IP

1. INTRODUCTION

Internet Protocol (IPv6 or IPng) is the cutting-edge time of IP and it is the successor of IP structure 4 which is commonly used nowadays. The headway of IPv6 started in 1991 and was done in 1997 by the Internet Engineering Task Force (IETF), and was definitively used in 2004 when ICANN added IPv6 addresses to its DNS server [1].

Information moves between hosts in bundles across over networks, these parcels require tending to plans. Using IPv4 and IPv6 these bundles can recognize their sources and besides find their objectives. Every contraption on the Internet needs an IP address to talk with various devices, and the advancement of the Internet incited a prerequisite for another alternative for IPv4, in light of the fact that IPv4 can't give the required number of IP address far and wide [2].

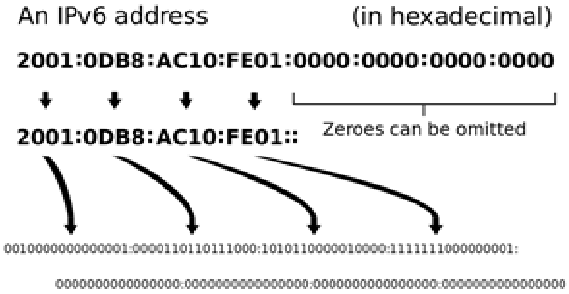


Fig 1 IPv6 Addressing

The area space in IPv6 is significantly greater than the area space of IPv4, and it went from 32 bits to 128 bits; figuratively speaking, it went from 4 billion conveys to 340 trillion of fascinating area [3]. IPv6 is proposed to give remarkable conveys to everyone on earth. This augmentation in area space won't just give progressively intriguing area anyway it will moreover make coordinating less requesting and cleaner in light of its dynamic tending to and increasingly clear IP header [2].

The IPv6 tending to structure is planned to give similitude existing IPv4 networks and allows the nearness of the two networks. IPv6 does not simply deal with the issue of lack that IPv4 is causing, anyway it is similarly updates and improves a part of the features that IPv4 has [4]. IPv6 uses 128 bits tending to plan that is addressed by

16-bit hexadecimal number fields confined by colons ":". Using this setup makes IPv6 less chaotic and screw up free. Here is an instance of an IPv6 address [5]:

2031:0000:130F:0000:0000:09C0:876A:130B

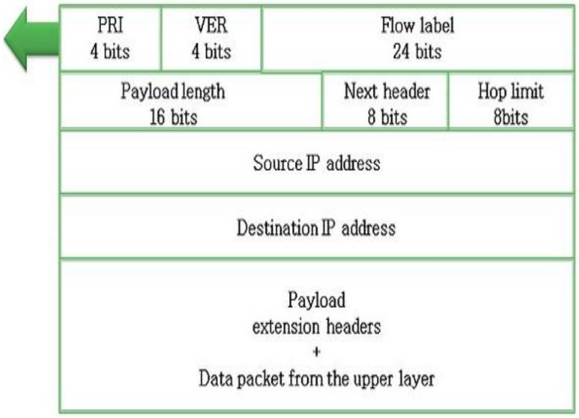


Fig 2 IPv6 Datagram

Additionally, this area can be contracted using a couple of principles like pressing the square of zeros to a single zero like this [5]:

2031:0:130F:0:0:9C0:876A:130B or 0000=0

Furthermore, dynamic fields of zero can be addressed by twofold colons "::", yet it is simply allowed once to use a twofold colon, so the above model will be contracted to this:[5].

2031:0:130F::9C0:876A:130B.

2. RELATED WORK

Shikhi Singh, Rohit Singh , 2017 [6] In current Internet steering design, the switch doesn't inspect or affirm the exactness of the source address passed on in the group, neither has it secured the state data when sending the bundle. Thusly the DDoS assaults with satirize IP source address can realizes causing the security issues. In this paper, their point is to shield the assailants from assaulting some spot outside the IPv6 edge organize with created source address in the fine granularity. In this makers have proposed a twofold security count, when scramble the message just as encode the key similarly as IP to which the message is to be send. The IP address is splited into the four areas and in like manner the key of 4 characters is used in their computation which is used for scrambling the IP by adding its ASCII motivating force to the all of the IP part and the last piece of the IP address is connected with the key in solicitation to also encode the key.

R. K. Murugesan and S. Ramadass, [7] Recently, IPv6 address the board has pulled in progressively vital intrigue and trade after recommendation were made to present contention by having a choice rather than the current game plan of IPv6 address scattering. This paper depicts an elective strategy for the apportionment of IPv6 addresses called the Country Internet Registry (CIR) appear. The proposed CIR model would serve despite the current Regional Internet Registry (RIR) show with the objective that the customers can investigate whom they wish to acquire their IPv6 addresses. Elective plans presented for IPv6 address assignment would support in giving an engaged area in IPv6 address the officials. This forceful condition would help-in making the RIR's to be progressively open to customer needs, help to vanquish oversight if any by the RIRs, and give overhauled administrations at a more affordable cost to the customers.

D. Gu, Y. Xue, D. Wang and J. Li, [8] makers have entered the transitional period some place in the scope of IPv4 and IPv6. Regardless, overseeing IPv4/IPv6 combination and advancement includes some absolutely new issues. Considering the organization issues amid IPv6 change, designers tried to propose IPv6 orchestrate virtualization engineering (VNET6). VNET6 has its very own organization show reliant on reflection. A headway count and autonomic control circle are unequivocally planned to automate provisioning of virtual resources and theoretical IPv6 advance administrations. The appraisal of their sending demonstrates that: VNET6, in a dynamic and autonomic overseeing way, can support IPv6 course of action and IPv6 change administrations.

J. G. Jayanthi and S. A. Rabara, [9] In the Internet, centers are recognized utilizing IP watches out for that depend upon their topological region. IPv4/IPv6 translation advancement includes address mapping some place in the scope of IPv6 and IPv4 center points and the methodologies used to disentangle protocols, where centers are in their specific IP variation of framework. A point by point think about is made on the IPv6 tending to design, distinctive IPv6 arranging frameworks and acquiring care-of-address. The examination evidently reveals that IPv6 tending to in IPv4 framework and the other path around are not considered. The paper brings up the need of IPv6 tending to in IPv4 orchestrate and propose another tending to framework with an obvious execution strategy, while not limiting any IPv6 portable center to meander just in IPv6 based frameworks. The as of late masterminded IPv6 address in the recommendation is suggested as P46CGA, which incorporates the enlargements to IPv6 stateless tending to instrument, cryptographic techniques, IPv4 switch address. Utilizing IPv4 switch address in IPv6 tending to in IPv4 mastermind helps substitute switches in the internet to perceive successfully the present zone of IPv6 center and to develop correspondence between them. The primary point of convergence of the recommendation is to enable an IPv6 portable center point to wander moreover into IPv4 based framework and get adjusted other than meandering in IPv6 based framework.

J. Lee, J. Bonnin, I. You and T. Chung,[10] IPv6 flexibility the administrators is a champion among the most testing examination subjects for empowering convenientce administration in the pending versatile remote organic frameworks. The Internet Engineering Task Force has been working for creating beneficial IPv6 convenientce the board protocols. As needs be, Mobile IPv6 and its developments, for instance, Fast Mobile IPv6 and Hierarchical Mobile IPv6 have been delivered as host-based compactness the officials protocols. While the host-based conveyability the administrators protocols were being improved, the framework based adaptability the board protocols, for instance, Proxy Mobile IPv6 (PMIPv6) and Fast Proxy Mobile IPv6 (FPMIPv6) have been institutionalized. In this paper, makers explore and dissect existing IPv6 flexibility the board protocols including the starting late institutionalized PMIPv6 and FPMIPv6. Makers perceive each IPv6 flexibility the board protocol's characteristics and execution markers by looking at handover exercises. By then, makers analyze the execution of the IPv6 adaptability the board protocols to the extent handover idleness, handover blocking probability, and bundle hardship. Through the coordinated numerical results, makers abbreviate examinations for handover execution.

S. Praptodiyono, R. K. Murugesan, I. H. Hasbullah, C. Y. Wey, M. M. Kadhum and A. Osman,[11] Internet Protocol variation six (IPv6) was arranged and made to handle the issue of exhaustion of current Internet address. IPv6 furthermore presents different points of interest including address auto-course of action framework which empowers host to self-produce its own one of a kind IPv6 address without the closeness of a DHCPv6 server. It is one part, among others, given by Neighbor Discovery Protocol (NDP). In any case, the protocol does not have a worked in security instrument and its messages were exchanged without security check as such leaving the framework feeble against abuse by toxic center points. A pernicious center point could aggravate or change the IPv6 address auto-age process that will leave the disastrous loss without an IP address required for correspondence or having a wrongly formed area. The NDP standard proposes either IPSec or SeND to confirm the instrument. Unfortunately, both security frameworks have been generally considered and were represented to have real drawbacks that limit their execution and gathering. This investigation proposes Trust-ND to confirm IPv6 address auto-plan instrument reliant on a conveyed trust framework. Investigation result shows that this framework is logically lightweight and uses less exchange speed while still prepared to fulfill the required security feature.

3. PROPOSED WORK

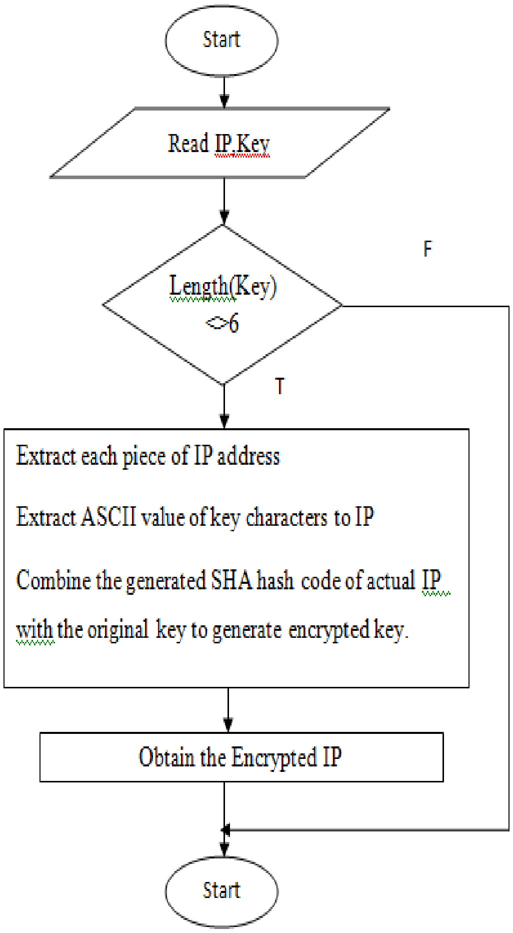

Start
Read IP,Key
Length(Key)
<>6
F
T
Extract each piece of IP address
Extract ASCII value of key characters to IP
Combine the generated SHA hash code of actual IP
with the original key to generate encrypted key.
Obtain the Encrypted IP
Start

Fig 3 IP Encryption Work

The proposed work works in the two phase, the first one focus on the encryption of the network ip address of type IPV6. The process of work is shown in the flowchart in fig 3.

The similar concept is also adopted for the decryption of the IP and the validation of the genuine IP is done using the SHA based algorithm.

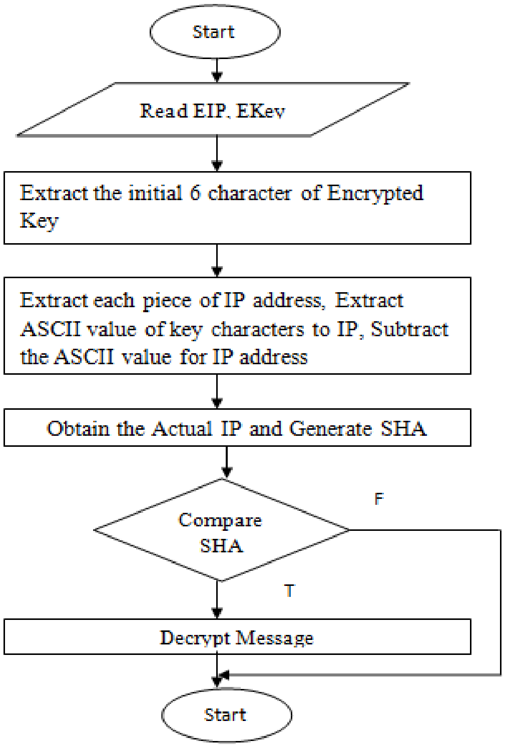
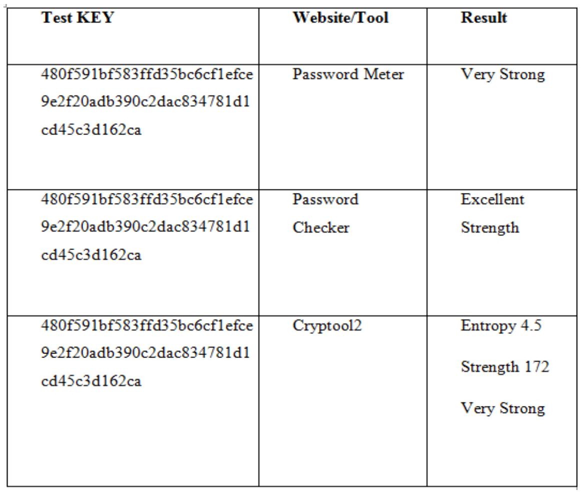

Start
Read EIP, EKey
Extract the initial 6 character of Encrypted Key
Extract each piece of IP address, Extract ASCII value of key characters to IP, Subtract the ASCII value for IP address
Obtain the Actual IP and Generate SHA
Compare SHA
F
T
Decrypt Message
Start

Fig 4 IP Decryption Work

4. RESULT ANALYSIS

The SHA 256 hash generated is validated using the various online and offline tool and the result of the same is presented in the table 1.



Test KEY	Website/Tool	Result
480f591bf583ffd35bc6cf1efce9e2f20adb390c2dac834781d1cd45c3d162ca	Password Meter	Very Strong
480f591bf583ffd35bc6cf1efce9e2f20adb390c2dac834781d1cd45c3d162ca	Password Checker	Excellent Strength
480f591bf583ffd35bc6cf1efce9e2f20adb390c2dac834781d1cd45c3d162ca	Cryptool2	Entropy 4.5 Strength 172 Very Strong

Table 1. Result Analysis

5. CONCLUSION

A champion among the most fundamental pieces of framework security is the various layers of security. There is no single group or structure that will offer completion affirmation against each hazard to your framework, so it is fundamental to try to use different layers of security for your framework. The proposed work utilizes the SHA put together approval with respect to the IPv6 address approval and proposed the SHA based approval of ASCII esteem moving content encryption. In the paper, the resultant figure content is attempted over the distinctive on the web and separated instruments for testing the nature of the figure and the result got are great.

REFERENCES

[1] Viney Sharma,"IPv6 and IPv4 Security challenge Analysis and Best- Practice Scenario",Int. J. of Advanced of Networking and Applications ,2010

[2] Kirandeep Kaur, Usvir Kaur,"A Review on IPv4 and IPv6 in Networking",International Journal of Computer Science And Technology,2016

[3] Olabenjo Babatunde, Omar Al-Debagy,"A Comparative Review Of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6)",International Journal of Computer Trends and Technology ,2014

[4] Dipti Chauhan and Sanjay Sharma, “A Survey on Next Generation Internet Protocol:IPv6",International Journal of Electronics and Electrical Engineering, 2014

[5] Monali S. Gaigole ,Prof. M. A. Kalyankar, "The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms”, International Journal of Computer Science and Mobile Computing,2015.

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

[7] R. K. Murugesan and S. Ramadass, "IPv6 address distribution: An alternative approach," 2010 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), Beijing, 2010, pp. 252-257.

[8] D. Gu, Y. Xue, D. Wang and J. Li, "IPv6 network virtualization architecture for autonomic management of IPv6 transition," 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, 2017, pp. 625-631.

[9] J. G. Jayanthi and S. A. Rabara, "IPv6 Addressing Architecture in IPv4 Network," 2010 Second International Conference on Communication Software and Networks, Singapore, 2010, pp. 461-465.

[10] J. Lee, J. Bonnin, I. You and T. Chung, "Comparative Handover Performance Analysis of IPv6 Mobility Management Protocols," in IEEE Transactions on Industrial Electronics, vol. 60, no. 3, pp. 1077-1088, March 2013.

[11] S. Praptodiyono, R. K. Murugesan, I. H. Hasbullah, C. Y. Wey, M. M. Kadhum and A. Osman, "Security mechanism for IPv6 stateless address autoconfiguration," 2015 International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT), Bandung, 2015, pp. 31-36.

[12] J. Hyun, J. Li, H. Kim, J. Yoo and J. W. Hong, "IPv4 and IPv6 performance comparison in IPv6 LTE network," 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), Busan, 2015, pp. 145-150.

[13] N. Chuangchunsong, S. Kamolphiwong, T. Kamolphiwong and R. Elz, "An Enhancement of IPv4-in-IPv6 Mechanism," 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, 2014, pp. 45-48.