International Journal For Technological Research In Engineering
Volume 6, Issue 6, February-2019 *ISSN (Online): 2347 - 4718*

SHA VALIDATION BASED ALGORITHM FOR ENCRYPTED IPV6 NETWORK ADDRESS AND TEXT MESSAGE SENDING

Kamini Singh[1], Sameeksha Chaudhary[2], Dushyant Singh[3]
[1]MTech. Scholar, [2,3]Assistant Professor
[1,2]Chandravati Group of Institutions, Bharatpur, Rajasthan, India,
[3]Vivekananda Global University, Jaipur.

Abstract: With the development of the cutting edge IT framework, there is the colossal development in the trading of the data in the electronic structure. With respect to the positive part of the innovation lies the negative angle additionally, in this day and age it is elusive the framework, one which isn't vulnerable to the programmer's assault. Thinking about this structures the premise of the paper work. In all regards the essential point of any secure communication framework is that the correct clients will get the right data one which is sent by the concerned recipient.

The proposed calculation works in the upgrade of the security , by not just chipping away at the assurance of the data which is to be sent to the beneficiary , but on the other hand is takes a shot at the encryption of the IPV6 based IP address. The calculation works, in the way of taking the key from the client which go about as the premise of the encryption of the IP address, by including the ASCII esteem with the IP address octet, and furthermore to frame the reason for the approval at the beneficiary end the key is additionally scrambled by connecting the SHA based hash code of the first IP address with the key, this further outcomes in qualities the key.

Keywords: IPV6 ,SHA ,Network Security

I. INTRODUCTION

Regardless of the very certainty that NAT in IPv4 decreased the measure of open IP tends to required in Associate in Nursing affiliation, NAT still has some security and execution issues. NAT being useful for customer server correspondence, for instance, email and net has issues concerning peer-peer correspondence [3].

IPv6 gives a start to end network affiliation that could be a sidekick peer framework utilized in applications like VOIP. It moreover has Associate in Nursing car style framework that enables clients to pass on self-sufficiently with no interest for a manual setup and what is more makes usage of IPSec necessarily inside the entireness of its correspondence. This assemble IPv6 more secure than IPv4 [1].

IPv6 can give greater space zone to a ton of reach and adaptability and this can concerning give boundless scope of IP regions and progressively beneficial frameworks for coordinative, subsequently these alternatives can give by and large passes on to each network invention and can have association through and through achieve capacity and higher network execution.

Furthermore, in light-load of the very certainty that IPv4 has less areas than IPv6, this can require the utilization of middle people and varying sorts of network mapping, on these lines expanding the risk in bundle sniffing through go-betweens by the by IPv6 contains a great deal of area region subsequently diminishing the utilization of delegates and in the long run expanding the element of security on the network. [1]

IPv6 offers an impressive area zone than IPv4. With 128 bits of IPv6 address permit with around 340 trillion, trillion, trillion areas. With such a concentrated scope of addresses, the requirement for NAT is feasibly appropriated with. At the reason once IPv4 was arranged security isn't the stress, in any case with IPv6, IPSEC is consolidated with the protocol with Associate in Nursing worthy key structure. IPv6 grants development for fresh out of the box new options by introducing another header position. By and by with this game plan treatment of IPv6 parcels could be a ton less confounded than IPv4. In IPv6 growth headers aren't prepared by each switch except for skip by hop elective and furthermore the affirmation field is in like manner discarded from the header, during this methodology making taking care of a ton of basic [2].

Auto style is that the fundamental piece of IPv6. IPv6 offers 3 styles of autoconfiguration-Stateful Autoconfiguration, destitute Autoconfiguration and each [4].Clients using IPv4 addresses use the Dynamic Host Configuration Proto0col (DHCP) [15] server each time they sign onto a network. This strategy is named stateful auto-plan. IPv6 supports a changed DHCPv6[16] protocol to help tantamount stateful auto-setup, by and by also reinforces destitute auto-course of action of center points that needn't bother with a server to collect locations, by and by uses change advancements to make an area. This makes a "connection and-play" condition and may enhance the board and association. IPv6 also allows modified area style and, sanctionative managers to renumber network delivers while not coming to all clients.

IPv6 what's more offers profitable and various leveled tending to and controlling establishment, designed - in security, Mobility, Multicast support, higher encourage for QoS and New protocol for neighboring center point affiliation. [3]

II. LITERATURE SURVEY

Shikhi Singh, Rohit Singh , 2017 [4] In current Internet directing engineering, the switch doesn't inspect or affirm the precision of the source address passed on in the group, neither has it secured the state data when sending the package. As such the DDoS assaults with caricature 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 figuring which is used for scrambling the IP by adding its ASCII motivator to the all of the IP part and the last piece of the IP address is connected with the key in demand to moreover encode the key.

R. K. Murugesan and S. Ramadass, [5] Recently, IPv6 address the board has pulled in increasingly essential intrigue and trade after recommendation were made to present competition by having a choice rather than the current course of action of IPv6 address scattering. This paper depicts an elective strategy for the appointment of IPv6 addresses called the Country Internet Registry (CIR) appear. The proposed CIR model would serve despite the current Regional Internet Registry (RIR) exhibit with the objective that the customers can investigate whom they wish to get their IPv6 addresses. Elective designs presented for IPv6 address assignment would support in giving an engaged space in IPv6 address the administrators. 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, [6] 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 during IPv6 change, designers tried to propose IPv6 orchestrate virtualization engineering (VNET6). VNET6 has its very own organization show reliant on reflection. A headway estimation and autonomic control circle are expressly planned to modernize provisioning of virtual resources and calculated IPv6 advance administrations. The evaluation of their sending demonstrates that: VNET6, in a dynamic and autonomic overseeing way, can support IPv6 game plan and IPv6 change administrations.

J. G. Jayanthi and S. A. Rabara, [7] In the Internet, center points are recognized utilizing IP watches out for that depend upon their topological region. IPv4/IPv6 elucidation development includes address mapping some place in the scope of IPv6 and IPv4 center points and the techniques used to decipher protocols, where center points are in their specific IP variation of framework. A point by point mull over is made on the IPv6 tending to design, diverse IPv6 arranging frameworks and acquiring care-of-address. The examination plainly reveals that IPv6 tending to in IPv4 framework and the other route around are not considered. The paper calls attention to the need of IPv6 tending to in IPv4 orchestrate and propose another tending to framework with an unquestionable execution strategy, while not limiting any IPv6 portable center point to meander just in IPv6 based frameworks. The as of late masterminded IPv6 address in the suggestion is insinuated 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 interchange switches in the internet to perceive adequately the present zone of IPv6 center point and to develop correspondence between them. The principle point of convergence of the recommendation is to enable an IPv6 portable center to wind similarly into IPv4 based framework and get adjusted other than wandering in IPv6 based framework.

J. Lee, J. Bonnin, I. You and T. Chung,[8] IPv6 flexibility the officials is a champion among the most difficult examination subjects for empowering versatility administration in the expected portable remote natural frameworks. The Internet Engineering Task Force has been working for creating gainful IPv6 conveyability the board protocols. In like manner, Mobile IPv6 and its developments, for instance, Fast Mobile IPv6 and Hierarchical Mobile IPv6 have been delivered as host-based compactness the administrators protocols. While the host-based conveyability the administrators protocols were being enhanced, the framework based flexibility the board protocols, for instance, Proxy Mobile IPv6 (PMIPv6) and Fast Proxy Mobile IPv6 (FPMIPv6) have been institutionalized. In this paper, makers research and examine existing IPv6 adaptability the board protocols including the starting late institutionalized PMIPv6 and FPMIPv6. Makers perceive each IPv6 adaptability the board protocol's characteristics and execution markers by looking at handover exercises. By then, makers analyze the execution of the IPv6 flexibility the board protocols to the extent handover latency, handover blocking probability, and bundle incident. Through the coordinated numerical results, makers compress considerations for handover execution.

III. PROPOSED WORK

The proposed calculation chips away at the two sections , first the assurance of the IP address and besides the security of the message which is to be send. The primary period of the calculation will be utilized for scrambling the IPv6 IP address which takes the six characters key and the including the ASCII estimation of the extricated characters of the key will produce the new encoded IP address and the key is likewise additionally scrambled by connecting the SHA hash code of the first IP address with the key, which will be utilized for approving at the recipient end. The text message is likewise utilized encoded utilizing the ASCII moving method and SHA code is additionally utilized in the approval procedure.

The usage work is performed on the Matlab r2011a. The reproduction of the base administrative work and the proposed work is finished by structuring the GUI. The GUI part of the matlab simply let us to make the screens by hauling the controls on the workspace. The structures which we make in the matlab are known as the figures.

MATLAB® applications square measure independent MATLAB programs with interface front completes that modernize A task or check. The interface usually contains controls, for example, menus, toolbars, gets, and sliders. Different MATLAB things, for example, Curve Fitting Toolbox™, Signal procedure Toolbox™, and framework Toolbox™ consolidate applications with custom UIs. You'll

have the capacity to in like manner manufacture your own custom applications, together with their relating UIs, for others to use.

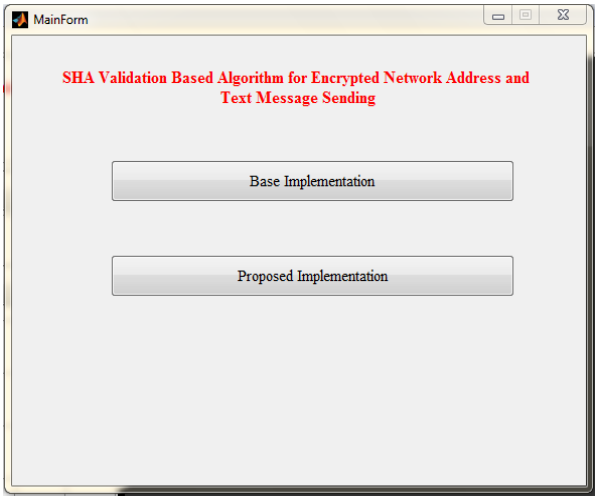

Fig. 1 Main Screen

Fig 1 demonstrates the fundamental screen which will be utilized for the execution start up work. The primary screen contains the two catches, one is for beginning up the base execution work and another is for beginning up the proposed usage work.

Fig 2 demonstrates the Base encoding IP process in which the contribution of IPv6 6 octet is given and utilizing the settled length 6 characters keys. At that point the ASCII estimation of the 6 characters keys is figured and included with the octet of the IPv6 address and the produced qualities will frame the encoded IP address. At that point the SHA calculation is utilized for age of the hash code which is then joined with the first key so as to frame the scrambled key.

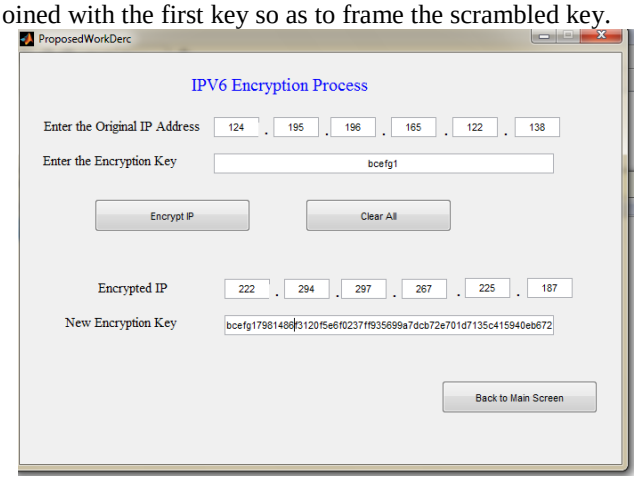

Fig 2 Proposed IP Encryption Process

Fig 3 demonstrates the text encryption process in the base work which scrambles the string utilizing the encrpytion calculation which included +3 in the every character ASCII incentive to create the new encrpyted characters and demonstrates the cipher textin the text box , after the cipher text is gotten , the SHA code of the first plain text is likewise produced which is utilized for the approval procedure at the beneficiary end , then the encoded IP ,the scrambled message , Hash code is send through some legitimate secure channel.

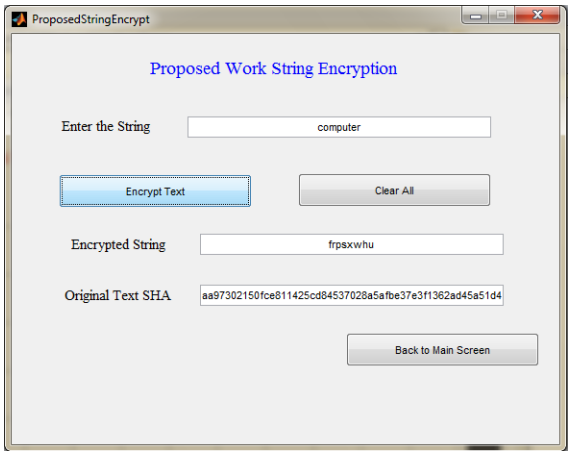

Fig 3 Proposed Message Encryption

IV. RESULT ANALYSIS

The result analysis is done by comparing the encryption key via various tools and websites for the key strength analysis

Table 1. Result Analysis

Test KEY	Website/Tool	Result
abcd347a990194cef7aee64e713ce7a85e7bf829a112ae161356937b72bb07786c4670	Password Meter	Very Strong
abcd347a990194cef7aee64e713ce7a85e7bf829a112ae161356937b72bb07786c4670	Password Checker	Excellent Strength
abcd347a990194cef7aee64e713ce7a85e7bf829a112ae161356937b72bb07786c4670	Cryptool2	Entropy 4.5 Strength 172 Very Strong

V. CONCLUSION

Network security is the any confirmation of access, misuse, and hacking of archives and lists in a PC sort out system. Without a doubt the most essential threats to a framework fuse diseases, worms, spyware, adware and data misrepresentation. A champion among the most crucial parts of framework security is the diverse layers of security. There is no single pack or structure that will offer completion affirmation against each hazard to your framework, so it is basic 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 text encryption.

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

REFERENCES

[1] Priya Bali,"A Detail Comprehensive Review on IPv4-to-IPv6 Transition and Co-Existence Strategies",International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 4, April 2015

[2] 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 (IJCTT) – volume 13 number 1 – Jul 2014

[3] Mohd.Khairil Sailan1, Rosilah Hassan2, Ahmed Patel3,"A Comparative Review of IPv4 and IPv6 for Research Test Bed",International Conference on Electrical Engineering and Informatics,2009

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

