International Journal For Technological Research In Engineering
Volume 5, Issue 1, September-2017 *ISSN (Online): 2347 - 4718*

A NOVEL APPROACH OF SECURITY BY DOUBLE ENCRYPTION USING SYMMETRIC KEY IN IPV6

Rakshanda Jibi[1], Mr. Ram Lal Yadav[2]
[1]M. Tech scholar, [2]Asst. Professor
Computer Science and Eng., Kautilya Institute of Technology & Engineering, Jaipur Rajasthan, INDIA

Abstract: Because there is increase in the trend of the data exchange by the electronic system, the need of information security has become a compulsion. The most important concern in the communication which is between sender and receiver is the security of the information which is to be transmitted. To get rid of the intruders various cryptographic algorithms are used for example: AES, DES, Triple DES, etc. Security is the utmost requirement in every aspect of our life. In the case of network, the security is must and there are number of algorithms and concepts that are proposed in order to enhance the security. In the similar fashion we have also produced the light weighted algorithm to enhance the security mechanism, in which we have encrypted the IP address, Key and message for double protection of the system. In order to provide double security, we have encrypted IP address as well as data.

I. INTRODUCTION

This current internetworking protocol [11], IPv4, inevitably will be notable satisfactorily bolster extra hubs and the necessities of the new applications. IPv6 is another network protocol whose components enhanced versatility and directing security, simplicity of-setup, and highest executions contrasted with IPv4. Tragically, IPv6 is inconsistent with IPv4 and to utilize new protocol will oblige changes to the product in each networked gadget. IPv4 systems, be that as it may, are universal and are not going to leave "over night" as the IPv6 systems are come in. Therefore, it is significant to create move components that endue applications to keep working while the hosts and the networks are being redesigned. One planned system is to translate IP headers as they go among IPv4 and IPv6 networks [3]. The prerequisite of header translation is to remain unambiguous to applications and network. In this paper we exhibit two forms of IPv6/IPv4 translators that point out these troubles. The primary variety utilizes unique IPv6 addresses, as proposed in [4], to effectively translate parcels directly for all applications. Lamentably, these unique IPv6 addresses also requires IPv6 switches to provide uncommon courses to them, which is an awful thought since it makes more state for the switch to keep up [4]. The second variety keeps up an express mapping among IPv4 and IPv6 addresses, in this way this is ready to use standard IPv6 addresses that don't need any extraordinary treatment by IPv6 switches. Its disadvantage is that IP-address installed in a few applications information stream, for example, FTP, it must be refreshed also so the translation will be totally straightforward. We have manufactured an IPv6/IPv4 network address and protocol translator as a gadget driver to be run in the Windows NT working framework [15]. Our test conditions comprises of the translator as a portal among IPv6 and IPv4 hosts associated with some Ethernet sections, and it cause a little execution overhead. Through some IPv6 and IPv4 hubs communicating by means of the translator, we measured TCP bandwidth of 7210 Kbytes/sec and roundtrip bundle latencies of 424 microseconds more than 100Mbit/sec Ethernet links.

1.1 Network Address and Protocol Translation

The address and protocol translation displayed in this segment empowers both the compatibility between hubs in an IPv4 site with hubs in the IPv6 network, and between the hubs in an IPv6 site with hubs in an IPv4 hubs. Figures 1 and 2 represent these situations, and the accompanying sections portray them in more detail.

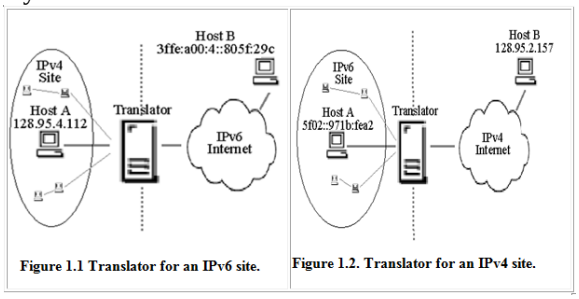

Figure 1.1 Translator for an IPv6 site. Figure 1.2. Translator for an IPv4 site.

Figure 1.1 delineates a translator of an IPv6 site communicating with the hubs in an IPv4 network.

The interior steering of the IPv6 site must be designed with the end goal that bundles expected for IPv4 hubs course to the translator. Hosts in the IPv6 site send parcels to hubs in the IPv4 network utilizing IPv6 addresses that guide to individual IPv4 hosts. For this situation, an outline introduced in [4] recommends that IPv6 hubs utilize an IPv4-perfect IPv6 address as their own address and an IPv4-mapped IPv6 address when interacting with IPv4-just hubs. An IPv4-perfect IPv6 address holds an IPv4 address in the low-arrange 32-bits, with a one of a kind high-arrange 96-bit prefix of 0:0:0:0:0:0(all zero bits), and dependably distinguishes an IPv6/IPv4 or IPv6-just hub; they never recognize an IPv4-just hub. Essentially, an IPv4-mapped IPv6 address recognizes an IPv4-just hub and its high-arrange 96-bits bear the prefix0:0:0:0:0:FFFF. The address of any IPv4-just hub might be mapped into the IPv6 address space by prefixing0:0:0:0:0:FFFF to its IPv4 address. The advantage of this approach is that the translator can be stateless. In any case, paying little respect to the 96-bit IPv6 prefix that is utilized to delineate the IPv4 and IPv6 address areas despite everything it stays important to distinguish a

host in the IPv6 site with an one of a kind IPv4 address. That is, in Figure 1, for Host B to speak with Host A requires an IPv4 address that can be steered through the IPv4 Internet. To beat this constraint a stateful translator could multiplex a few IPv6 hosts onto a solitary, universally novel IPv4 address utilizing the TCP/UDP port translation procedure depicted in [2].

II. LITERATURE REVIEW

J. Sagisi, J. Tront and R. M. Bradley[1]: This work displays the proof of idea usage for the main equipment based outline of Moving Target Defense over IPv6 (MT6D) in full Register Transfer Level (RTL) rationale, with future sights on an inserted Application-Specified Integrated Circuit (ASIC) execution. Commitments are an IEEE 802.3 Ethernet stream-based in-line network bundle processor with a specific Complex Instruction Set Computer (CISC) direction set architecture, RTL-based Network Time Protocol v4 synchronization, and a measured crypto engine. Customary static network addressing permits attackers the mind boggling favorable position of setting aside opportunity to arrange and execute assaults against a network. To counter, MT6D gives a network have muddling technique that offers network-based keyed access to particular hosts without changing existing network foundation and is an incredible technique for ensuring the Internet of Things, IPv6 over Low Power Wireless Personal Area Networks, and high esteem all around routable IPv6 interfaces. This is finished by crypto-graphically changing IPv6 network addresses at regular intervals in a synchronous way at all endpoints. An outskirt entryway gadget can be utilized to capture choose parcels to inconspicuously play out this activity. Software driven usage have postured many difficulties, in particular, consistent code upkeep to stay agreeable with all library and kernel conditions, the requirement for a host figuring platform, and not as much as ideal throughput. This work tries to defeat these difficulties in a lightweight system to be produced for useful wide organization.

K. Zeitz, M. Cantrell, R. Marchany and J. Tront[2]: As the utilization of low-power and low asset installed gadgets keeps on expanding drastically with the presentation of new Internet of Things (IoT) gadgets, security techniques are fundamental which are perfect with these gadgets. This examination progresses the information in the territory of digital security for the IoT through the exploration of a moving target barrier to apply for limiting the time attackers may direct surveillance on inserted systems while considering the difficulties
displayed from IoT gadgets, for example, asset and execution requirements. We present the plan and enhancements for a Micro-Moving Target IPv6 Defense including a description of the methods of operation, required protocols, and utilization of lightweight hash calculations. We likewise detail the testing and approval potential outcomes including a Cooja reproduction configuration, and portray the bearing to additionally upgrade and approve the security technique through substantial scale recreations and equipment testing taken after by giving data on other future contemplations.

W. Sun, C. Gao and J. Sun[3]: Through the presentation of mobile IP useful substances, the paper expounded on the operation mechanism of mobile IPV4. As indicated by mobile IP mechanism, the paper break down the explanations behind the development of mobile IPV4 triangular steering, and depict a technique to comprehend the triangular directing, On the premise of IPV6 idea, the paper investigation the mobile IPV6, at that point talk about the IPV6 development of the working mechanism that consolidated with the working mechanism of mobile IPV4, and near examination of the contrasts between mobile IPV4 and mobile IPV6, at that point explained IPV6 quality favorable position as far as taking care of the triangular steering issue, Through the Micro-mobility protocol examination, based on IPV6 quick exchanging technology, the paper proposed a quick exchanging technology of Micro-mobility protocol presented in mobile IPV6.

M. Idri[4]: Mobile networks are moving into the 5G which is imagined to confront different unpredictability of network management caused by the increasing information traffic demand, various wireless conditions, and multiple administration necessities. The necessities are solid to propose new network architecture planning to meet heterogeneous administrations demands originating from different technologies, for example, LTE, WiFi and past. It is then testing to handle the mobility management and all the more particularly vertical handovers which expect to keep up continuous session. As a proposed technology, Software-defined network (SDN) that licenses network administrators to effectively acquaint new administrations and with disentangle network management. Adding to this, Distributed Mobility Management (DMM) which is rising as another pattern to diagram future mobile network architectures with a specific end goal to defeat the brought together part of the current mobile network. Due to the predicted mastery of IPv6, a consolidated arrangement is examined to disentangle clients' mobility and to guarantee the QoS of various applications.
Based on SDN and DMM, IPv6 Routing Header will be the fundamental recommended answer for ensure mobility management in heterogeneous network.

S. Thielemans, M. Bezunartea and K. Steenhaut[5]: New Long-Range radio technologies have as of late showed up in the IoT landscape. Joining the current communication protocols with these novel radio technologies could build the potential open doors and the differing qualities of utilization cases for Wireless Sensor Networks. In this paper, a usage of a LoRa based sensor platform that uses the Contiki OS is proposed, keeping in mind the end goal to empower standardized IPv6 LoRa communications. This improvement will permit to expand cutting edge steering protocols for WSNs (e.g. RPL), and to exploit this recently accessible radio technology. The possibility of the reconciliation is shown by displaying range estimations for a point-to-point interface between two Contiki-empowered LoRa bits.

G. Ruty, A. Surcouf and J. L. Rougier[6]: The exponentially developing stockpiling demands that industry currently confronts puts an immense weight on customary distributed stockpiling systems. Surely, the concurrently expanding amount of accessible video substance and video quality accompanies another arrangement of difficulties that current distributed systems experience serious difficulties meet. These challenges are for the most part the aftereffect of plan choices that, while pertinent for the underlying extent of those systems, wind up limiting their adaptability. In this paper, a brisk diagram of these ordinary plan choices is exhibited for two cases: Ceph and GFS (Google File System). A unique and IPv6-driven architecture is then portrayed, that presents none of the previously mentioned versatility limitations, and a first model of this architecture is contrasted with Ceph.

III. PROBLEM DESCRIPTION AND REQUIREMENT ANALYSIS

3.1. Need of Information Security

The network requires protection against malicious attackers and hackers. Network Security has two fundamental securities. The first one is the security of data information i.e. to secure the data from illegitimate access and failure. And the second one is computer security i.e. to secure the information and data and to hidden hackers. Hither network security does not only mean protection in only one network rather in any network or every network.

At present our requirement of network security splits into two necessities. First is the necessity of information security and second one is the necessity of computer security.

On cyberspace or any other network of the organization, numbers of important information are transfer every day. These data can be use improperly by attackers.

The security of the information is necessary because of the following under mention reasons.

1. To secure the confidential information users on the cyberspace. Other person cannot see or access it.
2. To secure the data from undesirable editing, unexpectedly or purposely by unauthorized users.
3. To secure the data from failure and check it that it is delivered to its destination securely. Manage the acknowledgement of the messages received by any node to protect from denial by sender in particular condition. For example suppose a client wants to purchase a few shares XYZ from the broader and then he refuse for the order after three days as soon as the rates go down. To restrict the user to send some message to other user on behalf of a third one. For example a user A for his own interest create a message including some favorable instructions and sends it to user B in such way that C receives the message as coming from C, the manager of the system.
4. To secure the message from unwanted delay in the transmission lines/route in order to deliver it to desire destination in time, in case of urgency.
5. To secure the information from drifting data packets or information packets in the network for non-finite long time and thus increase congestion in the line in case of destination machine fails to capture it because of some internal failures.

3.2 Security Contravention

Data and security contraventions are the result of breakdown in protecting the information leads to compromised unsecure data which leads to severe and devastating consequences. A contravention in a business leads to huge financial penalties, expensive law suits and loss of reputation and business. A contravention for individual can lead to identity theft and financial damage and credit rating. Recovering from information ruptures [12] can take years and the expenses are enormous. A current, very much advertised information rupture happened at the famous TJX apparel organization amid 2006/7, when more than 45 million credit/charge cards and about 500,000 records containing client names, government disability and drivers permit numbers were bargained. This information is accepted to have been traded off because of lacking security on their remote networks, leaving the information uncovered. The last expenses of the rupture are relied upon to keep running into the $100s of millions and potentially over $1 billion.

IV. PROPOSED WORK

In this thesis we have proposed a solution in order to double protect the whole system. In order to provide the double security, we have encrypted IP address as well as the data. In order to encrypt the IP address we have taken the key which will be of 4 characters in length. And it will encrypt the IP address by adding the ASCII value of each character to the each of the IP part. And the key is further encrypt and the last IP part will be concatenated in the key. Now to decrypt the IP , the process is the receiver when type the encrypted Ip with the Key , the first four characters of the key are first extracted and then decrypt the encrypted IP by subtracting the ASCII values and also the last part of the new IP is matched with the remaining characters of the encrypted key. And if they match then we proceed further.

4.2 Algorithm of Encrypting IP is as follows

Step 1: Read IP, KEY

Step 2: If Length (KEY) <> 4 then Exit by Giving Error Message

Step 3: Extract each part of IP address separated by. (period)

Step 4: Now find ASCII values of each of the four characters

Step 5: Add both the values to get the encrypted IP denoted by EIP.

Step 6: Now last IP part of our actual IP is extracted and concatenated with the KEY to form the new EKEY.

4.3 Algorithm of Decrypting IP is as follows

Step 1: Read EIP, EKEY

Step 2: Extract first four character of EKEY and find their ASCII values.

Step 3: Extract each part of EIP address separated by. (period)

Step 4: Subtract the both values to get the actual IP denoted by IP.

Step 5: Now last IP part of our actual IP is extracted and compared with the characters after the first four characters in the EKEY.

Step 6: If both match then we will proceed further.

4.4 Encrypting the Plain Text

Now the Message is also further encrypted and in this case

we will follow the following steps.
Step 1: Read PTEXT
Step 2: KEY initialized with
Dim KEY_128 As Byte() = {42, 1, 52, 67, 231, 13, 94, 101, 123, 6, 0, 12, 32, 91, 4, 111, 31, 70, 21, 141, 123, 142, 234, 82, 95, 129, 187, 162, 12, 55, 98, 23}
Step 3: IV initialized with Dim IV_128 As Byte() = {234, 12, 52, 44, 214, 222, 200, 109, 2, 98, 45, 76, 88, 53, 23, 78}
Step 4: CTEXT which is cipher text is formed.
4.5 Decrypting the Plain Text
Now the Message is also decrypted after the validation of IP and in this case we will follow the following steps.
Step 1: Read CTEXT
Step 2: KEY initialized with
Dim KEY_128 As Byte() = {42, 1, 52, 67, 231, 13, 94, 101, 123, 6, 0, 12, 32, 91, 4, 111, 31, 70, 21, 141, 123, 142, 234, 82, 95, 129, 187, 162, 12, 55, 98, 23}
Step 3: IV initialized with Dim IV_128 As Byte() = {234, 12, 52, 44, 214, 222, 200, 109, 2, 98, 45, 76, 88, 53, 23, 78}
Step 4: PTEXT which is plain text is formed.
Use the predefined statement (as prefigure in the sample code that follows) on the following namespaces:
• System
• System.Security
• System.Security.Cryptography
• System.Text
• System.IO
Because of these statements there is no need to qualify declarations from these namespaces later in your code. You have to use these statements before any other declarations.

```
using System;
using System.IO;
using System.Security;
using System.Security.Cryptography;
using System.Runtime.InteropServices;
using System.Text;
```

V. TESTING AND RESULTS ON BASE IMPLEMENTATION

5.1 PHP: Hypertext Preprocessor
PHP stands for PHP: Hypertext Preprocessor. PHP is a server-side scripting language, like ASP. PHP scripts are executed on the server. PHP supports many databases (MySQL, Informix, Oracle, Sybase, Solid, PostgreSQL, Generic ODBC, etc.). PHP is an open source software. PHP is free to download and use. PHP files can contain text, HTML tags and scripts. PHP files are returned to the browser as plain HTML. PHP files have a file extension of ".php", ".php3", or ".html".

5.2 MySQL
- MySQL is a database server
- MySQL is ideal for both small and large applications
- MySQL supports standard SQL
- MySQL compiles on a number of platforms
- MySQL is free to download and use

5.3 Registration Module
We will go to the double_security_algo and then create a new Registration by inserting username, selected password and particular e-mail Id and Click on Registration Save.

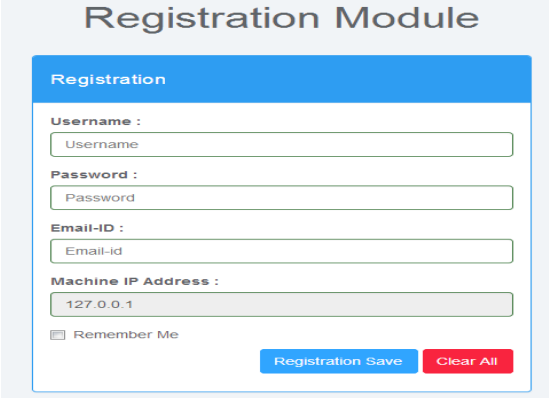

Fig. 5.1 Registration Form
After Click on Registration Save button our information has been successfully saved. A "Registration Saved successfully" message will show on the screen.

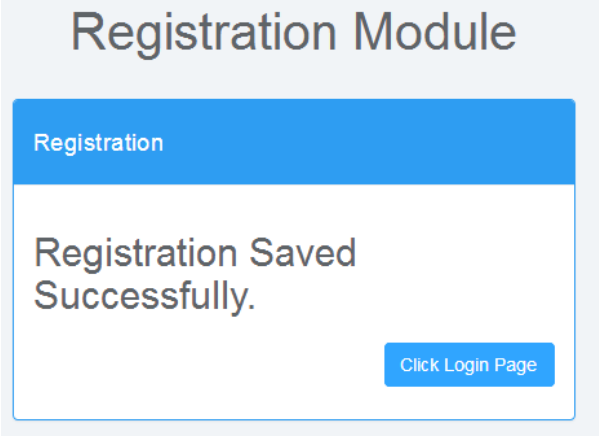

Fig. 5.2 Login Successfully Message
After click the "Click Login Page" button a login page will open.

5.4 Login Page
After Registration we will go to Login Page.

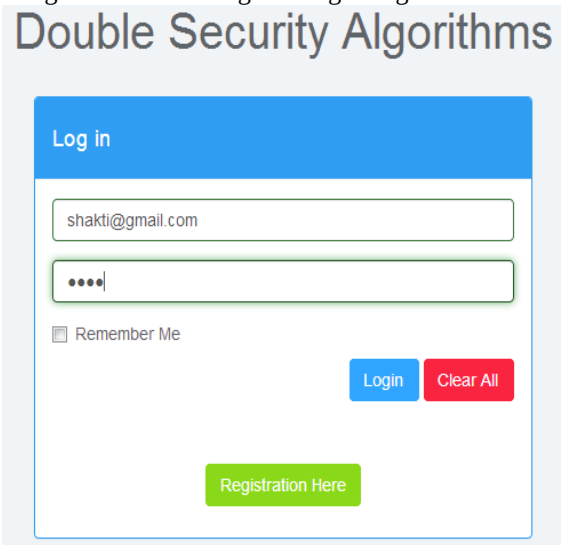

Fig. 5.3 Login Form page

Case 1: Login Failure: We have insert wrong e-mail id and password it will be not going to Home page and show message to insert right e-mail id and password.

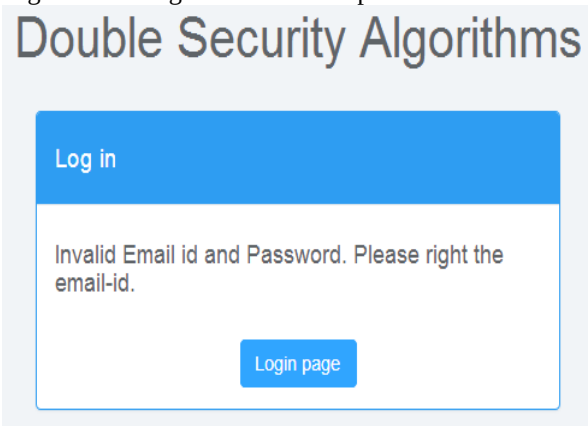

Fig. 5.4 Login Failed Message

Case 2: Correct Email id and Password: If Email id and Password is correct it will open the home page

5.5 Home Page

We are successfully Login in Double Security Algorithm and home page shows our Id with actual IP Address.

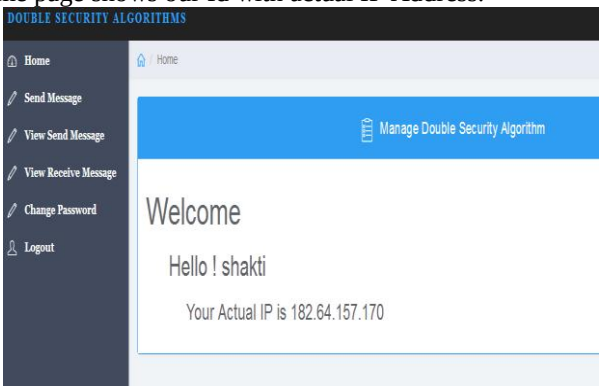

Fig. 5.5 Home Page

5.6 Send Message Form

After Login successfully there are many options in side menu. Here to send the message select a receiver ID whom we wish to send the message, then type max and min 4 characters key and then type the message.

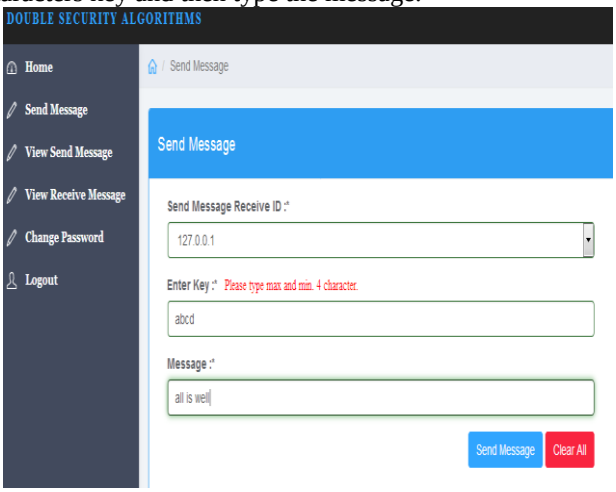

Fig. 5.6 Send Message Form

Case 2: Acknowledgement Message

After click the "Sent Message" button to the selected IP address an acknowledgement message will be received with ASCII Code.

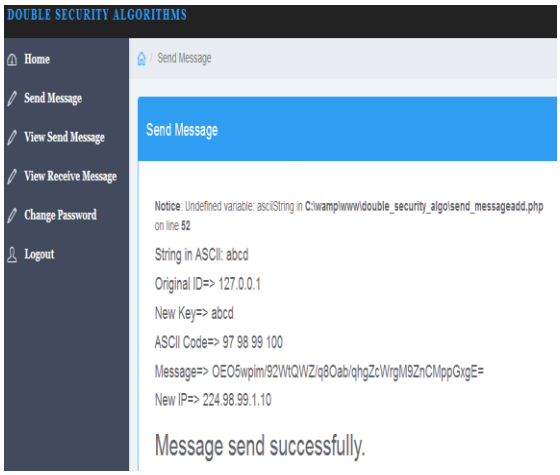

Fig 5.7 Acknowledgement Message

VI. CONCLUSION AND FUTURE SCOPE

Conclusion

We survey the best in class answers for handle security and privacy challenges in Device-to-Device communication. The checked on approaches traverse over an assortment of D2D prospects, for example, network communication, peer revelation, closeness services, and area privacy. Notwithstanding the traditional survey on security, we likewise give a point by point discourse on D2D privacy. We compress and contrast the current arrangements agreeing with security and privacy prerequisites. In light of the examination, we additionally determine "best practices" and recognize open issues that merit future research. Security is the utmost requirement in every aspect of our life. In the case of the network the security is must and there are number of algorithms and concepts are proposed in order to enhance the security. As for lessons took in, the significant contemplations incorporate device differing qualities, asset constraint, client motivation, arrangement deployability, prerequisite clashes, assessment tools and legitimate concerns. We trust that the exchange exhibited in this survey will fill in as a source of perspective guide for scientists and engineers to encourage the plan and usage of D2D security and privacy arrangements. In the similar fashion we have also produced the light weighted algorithm to enhance the security mechanism, in which we have encrypted the IP, Key and message to double protection of the system.

Future Scope

In the future work we will try to implement this algorithm hard wired that we will embedded this algorithm in the network monitoring systems itself so that the further software based implementation will not be required to implement this security. In light of the examination, we additionally determine "best practices" and recognize open issues of future search.

REFERENCES

[1] E. Prem, Wireless Local Area Networks, Aug 97, http://www.cse.wustl.edu/~jain/cis788-97/wireless_lans/index.htm
[2] X. Cong, Wireless ATM - An Overview, Aug 97, http://www.cse.wustl.edu/~jain/cis788-97/wireless_atm/index.htm
[3] G.H. Forman and J. Zahorjan, "The Challanges of Mobile Computing," Computer, April 1994
[4] D.F. Bantz, "Wireless LAN Design Alternatives," IEEE Network, March/April 1994, pp. 43-53.
[5] H. Ahmadi, A. Krishna, and R. O. Lamaire, "Design Issues in Wireless LANs," Journal of High Speed Networks, Vol. 5, 1996, pp. 87-104.
[6] T. F. La Porta, K.K. Sabnani, and R.D. Gitlin, "Challenges for Nomadic Computing: Mobility Management and Wireless Communications," Mobile Networks and Applications, Vol. 1, 1996, pp. 3-16.
[7] R. Bagrodia, W.W. Chu, L. Kleinrock, and G. Popek, "Vision, Issues, and Architecture for Nomadic Computing," IEEE Personal Communications, December 1995, pp. 14-27.
[8] K. Pahlavan, T.H. Probert, and M.E. Chase, "Trends in Local Wireless Networks," IEEE Communications Magazine, March 1995, pp. 88-95.
[9] E. Links. W. Diepstraten and V. Hayes, "Universal Wireless LANs," Byte, May 1994, pp. 99-108.
[10] B. Jabbari, et al, "Network Issues for Wireless Communications," IEEE Communications Magazine, January 1995, pp. 88-98.
[11] A.K. Salkintzis and C. Chamzas, "Mobile Packet Data Technology: An Insight into MOBITEX Architecture," IEEE Personal Communications Magazine, February 1997, pp. 10-18.
[12] R.H. Katz, "Adaptation and Mobility in Wireless Information Systems," IEEE Personal Communications, First Quarter 1994, pp. 6-17.
[13] K.C. Chen, "Medium Access Control of Wireless LANs for Mobile Computing," IEEE Network, September/October 1994, pp. 50-63.
[14] C.A. Rypinski, "Standards Issues for Wireless Access," Business Communications Review, August 1992, pp. 40-45.
[15] G. Fay, "Wireless Data Networking," International Journal of Network Management, 8 March 1992, pp. 8-17.
[16] D.J. Goodman, "Second Generation Wireless Information Networks," IEEE Transactions on Vehicular Technology, Vol. 40, No. 2, May 1991

