International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

Authentication of IOT Device Network Address with Implementation in Virtual Machine

S. Uma Mageshwari, R. Santhi

Abstract: ***The IOT is booming in this era, to make user convenience much better than before. The IOT devices involved for communication can be vulnerable by the intruder. During data transmission for the IOT devices, it must be authenticated with suitable methodology. The hackers spoof the address and pretend to be the actual communicator. The other party trust this spoofed address is the authorized person. Hence, this can be processed with the appropriate Cryptography algorithms. The proposed approach is the fusion of AES and ECDSA with implementation of Python code in Ubuntu Linux. The established code takes the Network Address (MAC – Media Access Control) of running host directly through OS, such that the Network address is encrypted. The verification of the Network address is demonstrated with Windows and Ubuntu Virtual Machine. Therefore, the developed code must be installed in IOT device to accomplish secure data transmission. The motto of this paper is to enlighten the security for Network address of IOT devices.***

Keywords: Cryptography, IOT, Network Address, Security.

I. INTRODUCTION

After analyzing the various existing methods, the address spoofing is the greatest challenge for data security.This is accomplished in preventing the spoofing of Network address. This paper highlights the encrypted Network address must be sent to the receiver and it is authenticated with the password to prove the identity of the user. This scenario is proved with IP based connection using SSH (Secure Socket Shell) protocol between two hosts. The reason behind of choosing SSH is cryptography protocol to have secure network access. The SSH is an application layer protocol that runs over TCP (Transmission Control Protocol) for remote connection. Hence, the communication can be established only with the authorized devices in the network. Thus, it provides the stronger security to the entire system.

A. IOT Architecture

The IOT architecture paves the way for communication between the devices with the Network address. The Network address plays a vital role in the architecture. Such addresss can be hacked and later the entire network will be poisoned. Therefore, it leads to lack of security. The IOT architecture[3] can be classified broadly into three categories namely,

- Three Layer Architecture(Perception, Network & Application)
- Four Layer Architecture(Perception , Support, Network & Application)
- Five Layer Architecture(Perception, Transport, Processing, Application & Business)

B. Security Attacks In IOT

There are many vulnerable attacks possible for IOT devices. But the proposed method take into account only three attacks namely, Man-in -Middle , Denial of Service and Spoofing of Address. In simple words, the denial of service means creating unnecessary Network traffic , Man-in -Middle attack leads to eavesdropping without the knowledge of communicators and Spoofing makes the attacker to grasp the network access may be partially or completely.

C. Cryptography Algorithms Used To Prevent Attacks

Among various cryptography algorithms, the most suitable algorithm identified is AES approved by NIST(National Institute of Standards and Technology) in US. The AES is used for encryption of Network address to accomplish confidentiality. ECDSA is used for signing and verifying the digital signature with the Network address for Authentication.

- DES(Data Encryption Standard)
- RSA algorithm(Rivest Shamir Adleman)
- AES(Advanced Encryption Standard)
- ECDSA(Elliptic Curve Digital Signature Algorithm)

D. Cryptography Keys

The keys in algorithms makes the code very protected. Such key size may contrast depends on the algorithm preferred for encryption and decryption process. The proposed approach emphasizes data encryption and digital signature keys. The different role of cryptographic keys is given below.

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
S.Uma Mageshwari*, Research Scholar, R& D Centre, Bharathiar University , Coimbatore, India.
Dr. R.Santhi, Research Supervisor, Bharathiar University, Coimbatore, India.

Table 1[2]: Difference Between Cryptographic Keys

Features	Data Encryption Key	Master Key	Root Key	Digital Signature Key	Key Encryption Key	Authentication Key
Purpose	Confidentiality	Encryption of Many keys	Authentication & Digital Signature Certificates	Verifying integrity of the message	Encapsulation of Secret Key	To prove the key is valid
Type	Symmetric or Asymmetric	Symmetric	Asymmetric	Asymmetric	Symmetric or Asymmetric	Symmetric
Size	AES (128 -256 Bits)	128 -256 Bits	256 – 4096 Bits	ECDSA (192 -512 Bits)	Based on the algorithm chosen	SHA- 2 (224 – 512 Bits)

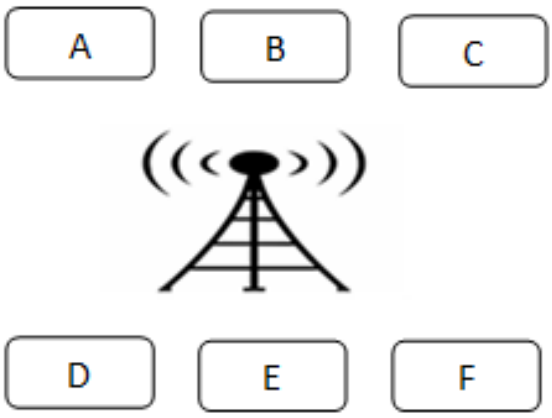


Fig 1: Sample Illustration of IOT devices interconnected

II. LITERATURE REVIEW

[5] Intruders Discovery: The communication architecture uses five layers for detecting the intrusion. This approach used the technique of finding IP and MAC address of an attacker with Interloper software. This software enables the Network architecture to work based on the concept of sending request and response for the request from host. This software helps to detect the unknown person trying to use the network. Only, the intruder's MAC address is logged in this software with the support of 'pyshark' and 'scapy' tools. Hence, the intruder's original logical address needs to be identified.

[6] ARP Harming: In this methodology, the ARP (Address Resolution Protocol) attack avoidance is worked out with external hardware component Arduino. The testing is carried out which outbreak the embedded controller of Arduino. The prevention is achieved with kali Linux which keeps track of packets of IOT node. The implementation of this approach is done in two steps. The first step is to screen the ARP packets with Virtual machine and analysed with installation of Wireshark on Ubuntu to obtain the attacker. The second step is about linking of IOT node and Virtual machine. Hence, VM can screen all the ARP data direct to IOT nodes. The 'arptable' tool has been used in Linux for malicious attack detection. This procedure can be used only for limited IOT devices.

[7] Dynamic IP Address: This method assigns the IP address for IOT devices and validating the device is done through Gateway. The Gateway stores the IP address and allocates to the device as on claim for communication. The DHCP (Dynamic Host Configuration Protocol) has been used for allocating dynamic address. The receiving packets are authenticated with the database table of IP address. If it doesn't match, then packets are rejected. This is reached with the technique of initiating communication with Gateway of adding optional data in IPV4 header. The optional data comprises of three parameters viz., Typ, Len and Val. The different values for Typ parameter make the difference in communication. If the Typ value is '1' then Gateway Announce, Typ value '2' means Address Demand, Typ value is '3' then Address Reply and Typ value '4' means Address approve. Therefore, with this approach IP address can be assigned dynamically but the MAC address can be reproduced by an intruder.

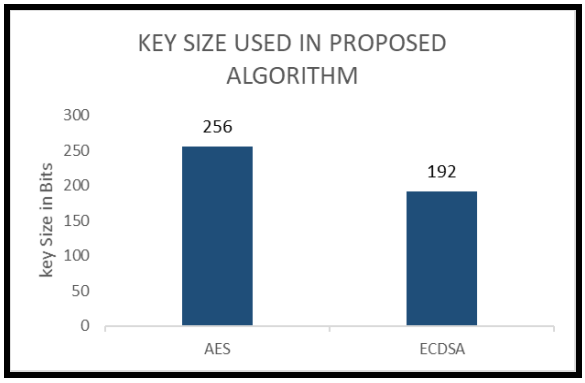
III. METHODOLOGY AND RESEARCH

[1] In the proposed algorithm, AES symmetric key and ECDSA asymmetric key are used to avoid spoofing of Network address before data transmission in the network. The hackers keep track of communication line and identify the Network address which in turn cause effects to the Network structure in terms of Confidentiality and Authentication. The python dependency such as "starbank-ecdsa" is installed. So, it requires 192 bits keys size for both signing and verifying of ECDSA algorithm. The traditional method adopts too long technique of preventing address Spoofing. But the proposed method is simple but forceful way of thwarting spoofing of Network address.

A. Description of the Proposed Algorithm

Step 1: Given the 12 -bit Network Address as an input of running host.
Step 2: Convert the input into 128 bits for AES algorithm.
Step 3: AES algorithm process it with key size of 256 bits.
Step 4: Network address is encrypted with AES key.
Step 5: Private Key of 192 bits is generated with ECDSA algorithm for the Network address signature.
Step 6: Network address is decrypted with AES key.
Step 7: Network address is verified with Public key of 192 bits for ECDSA algorithm.
Step 8: If the signature is valid, then the Network address will be decrypted.
Step 9: Display the 12 – bit Network address of running host.

Cryptography Algorithms	*Status*	*Purpose*	*Result*
AES	Existing Method	Confidentiality	Encrypt Network address of the host and Decrypt it with Authentication.
ECDSA	Existing Method	Authentication	
Fusion of AES & ECDSA	Proposed Approach	Confidentiality & Authentication	



AES : Symmetric key
ECDSA : Asymmetric key
(Signing & Verifying)

Fig 2: Key size Illustration

IV. IMPLEMENTATION AND RESULTS

The implemented python code is validated in the Virtual Machine with two hosts Linux (Sender) and Windows (Receiver). In this way, the Network address is authorized with the password on the receiver host. The following dependencies need to be installed with command "pip install" to make this code to run successfully. The dependencies are certify==2019.6.16, chardet==3.0.4, crypto==1.4.1, ecdsa==0.13.2, idna==2.8, Naked==0.1.31, pycrypto==2.6.1, PyYAML==5.1.1, requests==2.22.0, shellescape==3.4.1, starkbank-ecdsa==0.1.5 and urllib3==1.25.3.

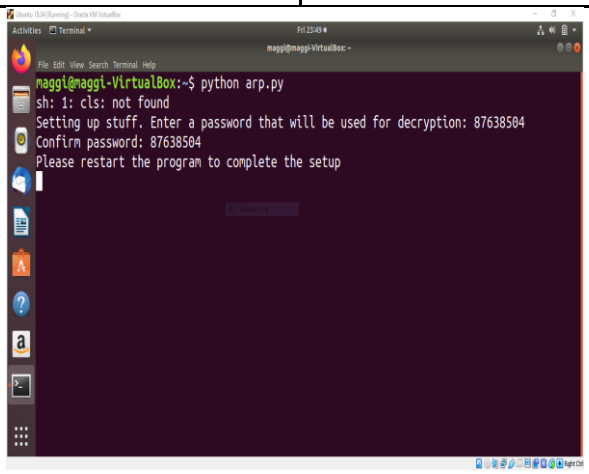


Fig 3: Host in Linux (Ubuntu) – Sender

The IP address of running host is identified with 'ifconfig' command. The windows OS uses the PuTTY application as a receiver. Using SSH protocol the IP address relates to windows. The performance metrics of executed code is identified with the parameters such as speed, CPU and size. The speed of the code is originating with the command "python -m cProfile filename.py" and CPU utilization time is found with python command "top -n 1". The proposed developed code is compatible with cross platform.

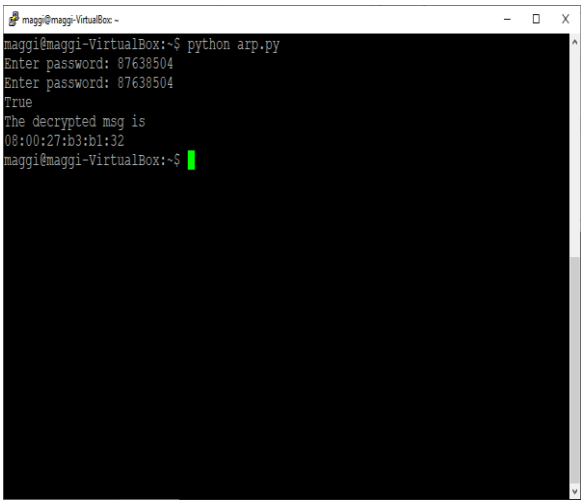


Fig 4: Host in Windows - Receiver

METRICS	VALUES
Speed	4.527 Seconds
CPU	1.9 Microseconds
Size	4.4 KB (4383 Bytes)

Table 3: Performance Analysis in VM

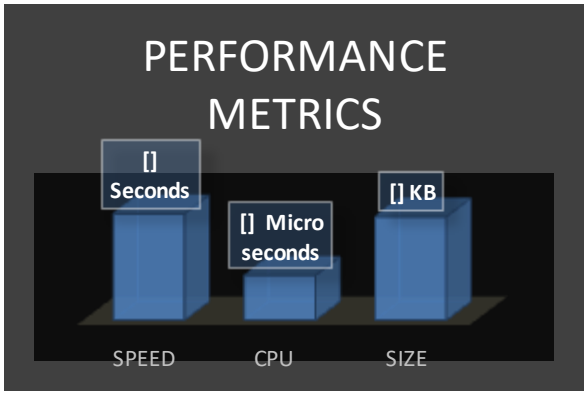
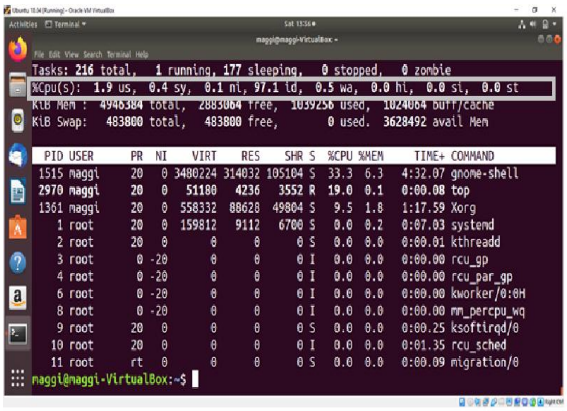


Fig 5: Pictorial Representation of Performance



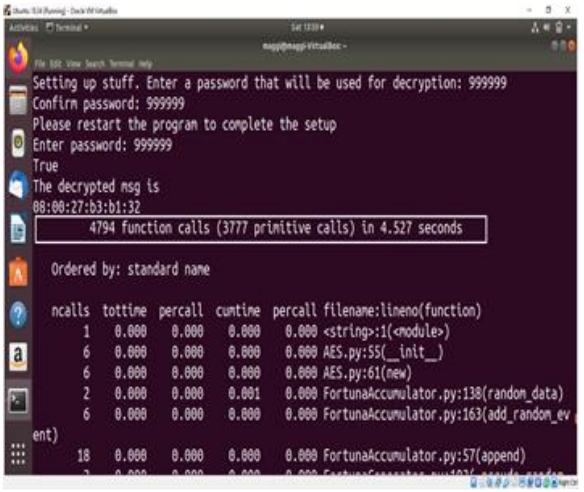


Fig 6: Performance Metrics are identified with Python Commands.

V. DISCUSSION

After scrutinizing the existing methods, to avoid address spoofing is done in tedious way. The existing related work keeps track on data packets flow during transmission, out of which, identified the attacker's details. But the proposed work makes the job easier by simply transmitting the device Network address in an encrypted form before starting up the communication between the IOT devices. Then, decrypt the same with authentication and only the authorised person can see their address. The key size used for password is only 64 bits for security. The running host network address is acknowledged directly from operating system with python commands. Hence, the intruder not able to spoof the address of IOT devices. The proposed work is robust tool of avoiding three attacks Man-in-Middle, Denial of Service and Address Spoofing. Therefore, the harmless and protected communication channel is established between the devices.

A. Features of the Proposed Method

- Framed Code is tested in Ubuntu Virtual Machine. So, it can be used in IOT Devices.
- Interoperability.
- Password Used for Authentication is dynamic.
- Before the communication initiates, the password can be fixed that moment between sender and receiver. So, no need to recollect the old password.
- Running host Network address is protected from the Intruder.
- The size of the password should be 64 bits (must contain 8 digits).
- Python dependencies can be installed directly with an Internet connection.
- Cost effective.
- Can be used in VPN and LAN.

VI. COMPARATIVE STUDY OF EXISTING METHODS WITH THE PROPOSED APPROACHzOF ARP SPOOFING FOR IOT

Table 4: Illustration of different Methodology adopted to prevent Spoofing for IOT by the authors.

riteria	Existing Method [5]	Existing Method [6]	Existing Method [7]	Proposed Approach [1]
Objectives	Identification of an Intruder	Prevention of ARP harming	Allocating IP address	Secure Network Address to avoid spoofing
Buzzwords	Authentication, Identification	ARP, Detection	Gateway, IP Addresses	Spoofing, Network Address
Methodology	Finds an attacker by monitoring the Network traffic.	Analysing the ARP packets to detect an Intruder	IP address is given to IOT device through Gateway	Authenticates Network Address before data transmission.
Focussed Attacks	1.Man -in -Middle 2.Botnets 3.Node Replication 4.Physical Attacks	1.Denial of Service 2.Man-in-Middle 3.ARP Poisoning	1.Man-in-Middle 2.ARP Spoofing 3.Denial of Service	1. ARP Spoofing 2.Denial of Service 3.Man-in-Middle
Tools	Interloper Python	Kali Linux Wireshark	Changes to be done in the IPV4 header	Python Ubuntu Linux
Limitations	Must find attacker unique IP address	Applicable to inadequate IOT devices	MAC address can be spoofed by the hackers	Password must be shared before sending the actual data

VII.FUTURE SCOPE AND DEVELOPEMNT

In the proposed approach, the four layers i.e., Physical, Data Link, Network and Transport layer involved for Encryption and Decryption of running host Network address. In future, it can be enhanced to involve the other layers too in the communication model for data security. The authentication of the sender is verified with the password before communication commences with the devices. So, this can be improved during the data transmission itself the encrypted Network address can be appended with data.

VIII. CONCLUSION

The proposed approach is implemented and authorized the Network address in the Virtual Machine. The communication between two hosts is provided with SSH protocol to achieve network access remotely and the host connection is given with the IP address. The speed of the implemented python code is measured in seconds and it needs very less storage space. Therefore, such code can be used in IOT devices as well as the passwords can be changed periodically without changing the instructions in the code. Thus, the IOT device can communicate and validates the identity on the receiver side. The implemented python code should be installed in both sender and receiver side of IOT devices. In this method, the Network address is protected, and the network cannot be accessed by the hacker. Thus, the proposed approach seems to be modest and resourceful way to avoid spoofing of Network address.

ACKNOWLEDGMENT

I would like to thank all my friends Mr.R. Pradeep, Mr.S. Sandeep, Mr. R. Mohan, Ms.N. Renuka and Ms. K. Priya for their guidance and support in my research work.

REFERENCES

1. S. Uma Mageshwari, Dr. R. Santhi," Implementation of ARP Spoofing for IOT devices Using Cryptography AES and ECDSA algorithms", IJRTE, ISSN: 2277 -3878, Vol. 8, Issue-2S11, Sep 2019.
2. https://www.cryptomathic.com/news-events/blog/classification-of%02cryptographic-keys-functions-and-properties
3. https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.mdpi.com%2Fsensors%2Fsensors1802796%2Farticle_deploy%2Fhtml%2Fimages%2Fsensors1802796g006.png&imgrefurl=https%3A%2F%2Fwww.mdpi.com%2F14248220%2F18%2F9%2F2796%2Fhtm&docid=SZWrscVp9h7QUM&tbnid=XKErfYfRznSKM%3A&vet=10ahUKEwioLKI0KPmAhVLX30KHd6BAL0QMwisASg1MDU..i&w=3248&h=2451&bih=598&biw=1341&q=layers%20in%20iot%20model&ved=0ahUKEwioLKI0KPmAhVLX30KHd6BAL0QMwisASg1MDU&iact=mrc&uact=8
https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.15207%2FJKCS.2016.7.4.039
4. Ch Mohan Kumar, T Rahul Ratna, S Geethika, S UdayKiran," Detection of Intruders in IOT Networks Using Interloper Software based on Authentication", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN:2278-3075, Volume -8, Issue -6, April,2019
5. Weihua Gao et.all., "ARP Poisoning Prevention in Internet of Things", 2018 9th International Conference on Information Technology in Medicine and Education", IEEE,2018.
6. S Rajashree, Soman K S, Dr. Pritam Gajkumar Shah, "Security with IP Address Assignment Spoofing for Smart IOT Devices", IEEE, 2018.

7. Mohammed Al-Shaboti, Ian Welch, Aaron Chen, Muhammad Adeel Mahmood, “Towards Secure Smart Home IOT: Manufacturer and User Network Access Control Framework”, 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications”.
8. Bidyut Jyoti Saha, Kunal Kumar Kabi, Arun, “Digital Image Encryption using ECC and DES with Chaotic Key Generator”, International Journal of Engineering Research & Technology (IJERT), ISSN:2278-0181, Vol.2, Issue 11, November -2013.
9. Chandu et.al., “Design and Implementation of Hybrid Encryption for Security of IOT Data”, 2017 International Conference on Smart Technology for Smart Nation, 2017 IEEE.
10. Sattar B.Sadkhan , Zainab Hamza, “ Cryptosystems used in IOT – Current Status and Challenges”, 2017 International Conference on Current Research in Computer Science and Information Technology(ICCIT), Slemani,Iraq.
11. Israr Ahmed et al., “Security in the Internet of Things (IOT), The Fourth Information Technology Trends (ITT 2017), Dubai,UAE,Oct., 25-26 2017, IEEE.
12. B.K.S Rajaram, Krishna Prakash. N, “Secure MQTT using AES for Smart Homes in IOT Network”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Vol.8, Issue 5S March 2019.
13. Lavisha Sharma, Anuj Gupta, “Image Encryption Using Huffman Coding for Steganography, Elliptic Curve Cryptography and DWT for Compression”, International Journal of Advance Research, Ideas and Innovations In Technology (IJARIIT), ISSN:2454-132X, Vol.2, Issue 5,2016.
14. Ankit K.Dandekar, Sagar Pradhan, Sagar Ghormate, “Design of AES□512 Algorithm for Communication Network”, International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395- 0056,p-ISSN: 2395-0072,Vol.03, Issue 05,May 2016.1 16.
15. B.T. Geetha, Dr.M.V. Srinath, “A study on various Cryptographic Key Management and Distribution system in Secure Multicast Communications”, 2012, IEEE, DOI:10.1109/MNC Apps.2012.18.

AUTHORS PROFILE

Dr. R. Santhi MCA., MS., M.Sc., M.Ed.., M.Phil., Ph.D. Three Decades in the field of Education from Teacher to Dean and Principal. Former General Secretary, AMTI. Authored a book on Design and Analysis of Algorithms. Presented papers in many Conferences. Guiding many Ph.D. scholars.

S. Uma Mageshwari M.Sc., M.B.A., M.Phil., PGDCA., SET. Professor, more than 10 years of Teaching Experience in Department of Computer Science. Area of Interest in Cryptography. Published eight papers in UGC approved Journal and Scopus. Pursuing a Ph.D. at Bharathiar University, Coimbatore.