Implementation of ARP Spoofing for IOT Devices Using Cryptography AES and ECDSA Algorithms

S. Uma Mageshwari, R. Santhi

Abstract— The Internet of Things is the network of numerous devices and communicate with an internet by using the IP address. The IOT objects shares the information using wireless connection. During the data transmission, that can be distorted by the Hackers by knowing their IP address. In IOT (Internet of Things), the wireless communication between the devices makes the users to be vulnerable. So, the hackers may spoof the MAC address of the communicating devices. The receiver MAC address is identified and then false MAC (Media Access Control) address is created by the hacker. Then, attackers replaces the original MAC address in the ARP (Address Resolution Protocol) table of the sender. So,the hackers may impersonate like the sender. Therefore, Cryptographic algorithms like AES (Advanced Encryption Standard) for confidentiality and ECDSA (Elliptic Curve Digital Signature Algorithm) for Authentication are applied in the proposed algorithm to safeguard the data as well as the devices from the hackers. The following attacks such as Man-in-the-Middle, Denial -of -Service (DOS) and ARP spoofing are strongly prevented in the proposed algorithm. Thus, the implementation of an algorithm is carried out in Ubuntu Linux environment with installing Python dependencies. This algorithm affords an efficient way to thwart ARP (Address Resolution Protocol) spoofing by the hackers for IOT devices.

Keywords: AES, ARP, DOS, ECDSA ,IOT and Man in the Middle Attack.

I. INTRODUCTION

IOT is the interconnection of physical devices over the network and set in with electronics, software and sensors. Thus, it makes the data to be exchanged among the devices efficiently. The devices and computers are connected with several technologies such as RFID, Wi-Fi etc…The IOT makes the devices to be connected, controlled and managed in the network. Therefore, it makes the job easier than before. But the communication through wireless devices are easy to change the network traffic. To avoid the IOT devices sniffing by the hackers, the three attacks namely Man-in-the-Middle, Denial –Of- Service and ARP spoofing need to be detected.

A. Man –In –The -Middle Attack

The Man-in-the-Middle (MITM) attack is a type of eavesdropping in which the conversation between the communicating parties will be in control of the attacker. The MITM attack mishandles the electronic transactions or data transfer between the legitimate people. The MITM is the widespread attack for the IOT devices and the attacker impersonate like the authentic user.

The Man-in-the -middle attacks can be done in several ways such as,

ATTACKS	**MEANING**
DNS SPOOFING	IP addresses has been changed by the hacker.
SSL HIJACKING	To get the encrypted data by the attacker
ARP POISONING	To create the fake MAC address by an intruder
HTTPS SPOOFING	User thinks interacting with a legitimate websites but in actual give away the information to malicious person
WIFI EAVESDROPPING	To steal the data in an unsecured wifi network

Table 1: MITM Attacks

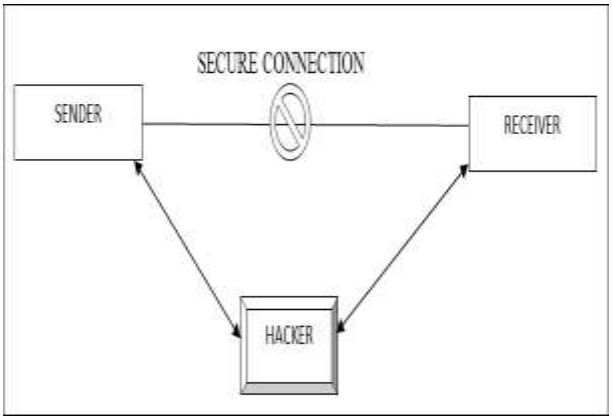

Fig-1: MAN –IN –THE - MIDDLE ATTACK

B. Denial of Service

The DOS attack makes the network to be unavailable for the genuine user by flooding the network traffic. The Denial –Of -Service forbids the standard communication by overloading the target host which in turn degrade the performance of the system. The DOS attack harm the number of IOT devices by using a worm.

Revised Version Manuscript Received on 10, September 2019.

S. Uma Mageshwari, Research Scholar, R& D Centre, Bharathiar University , Coimbatore, Tamil Nadu, India.

Dr. R. Santhi, Research Supervisor, Bharathiar University, Coimbatore, Tamil Nadu, India.

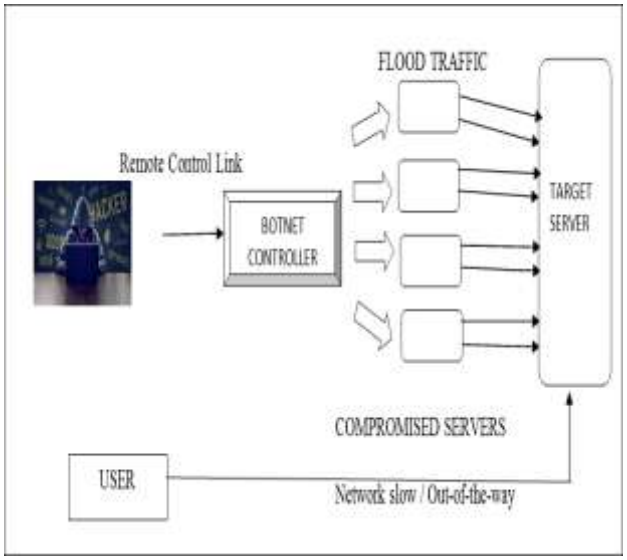

Fig -2: DISTRIBUTED DENIAL –OF-SERVICE ATTACK

C. Arp Spoofing Attack

- To communicate in a network, a sender device must know the IP address and MAC address of the receiver. The MAC address is also known as physical address.
- Sender will send ARP request message to the receiver. It will respond MAC address with ARP response message.
- The sender stores MAC in ARP table against the receiver. The receiver IP address (logical address) must be associated with MAC address to transfer the data.
- The hackers may communicate vulnerable to the sender and get the IP address of the receiver. The attacker sends unsolicited ARP response message in which the MAC address of the receiver has been changed in the ARP table of the sender.
- The sender communicates to the receiver with wrong MAC address but it goes to the attacker host. Therefore, the Hackers sniffs and able to control the network traffic.

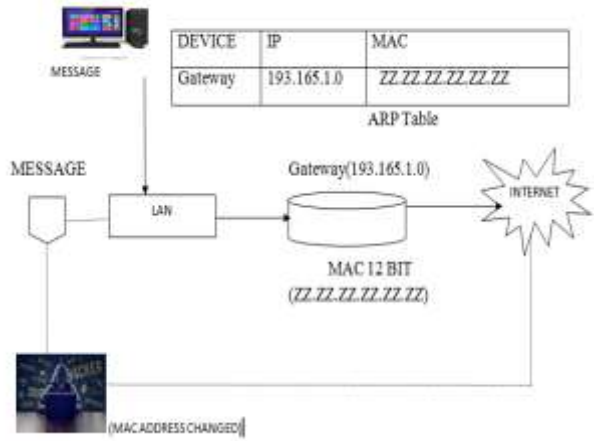

Fig -3: ARP SPOOFING IN LAN NETWORK

II. LITERATURE REVIEW

[4] B.K.S Rajaram, Krishna Prakash. N: The IOT for smart homes is accomplished using AES algorithm with MQTT protocol. It is implemented in Raspberry pi for smart home structure in the hardware.

[5] Ankit K.Dandekar, Sagar Pradhan, Sagar Ghormate: The AES algorithm use 512 bits for encryption/decryption process. This paper enhances the security for the network.

[6] Lavisha Sharma, Anuj Gupta: The image is encrypted using ECC and DWT (Discrete Wavelet Transform) procedure for image compression. The MATLAB software is used for implementation.

[8] Deepika Khambra,Poonam Dabas: The AES algorithm is used to secure data in IOT. The proposed mechanism is implemented in MATLAB and the performance of proposed algorithm is examined.

[10] Chandu et.al.,The hybrid implementation of AES and RSA is used to secure IOT data. The result is tested with Xilinx ISE –Design 14.5 software. The Encryption/Decryption of RSA is done in MATLAB.

III METHODOLOGY

A. AES(Advanced Encryption Standard)

[2] AES encryption standard is formulated by National Institute of Standards and Technology (NIST), USA. The AES designers are Vincent Rijmen and JoanDaemen. The AES algorithm is a block cipher symmetric key algorithm. The AES algorithm accepts 128 bits of data as plaintext. Using the symmetric key, the data is encrypted and produces the ciphertext. The ciphertext creates the plaintext by using the same key. This AES algorithm is best well-matched for confidentiality. The AES key sizes can be 128,192 and 256 bits and their respective rounds are 10, 12 and 14. The four tasks performed in AES are as follows,

- SubBytes - Substitutes an element of S-box matrix
- ShiftRows - Rows of the block moved in left side
- Mix Columns - Block is multiplied with a static matrix
- Add Key Matrix - Each byte is XORed with the respective element of the key

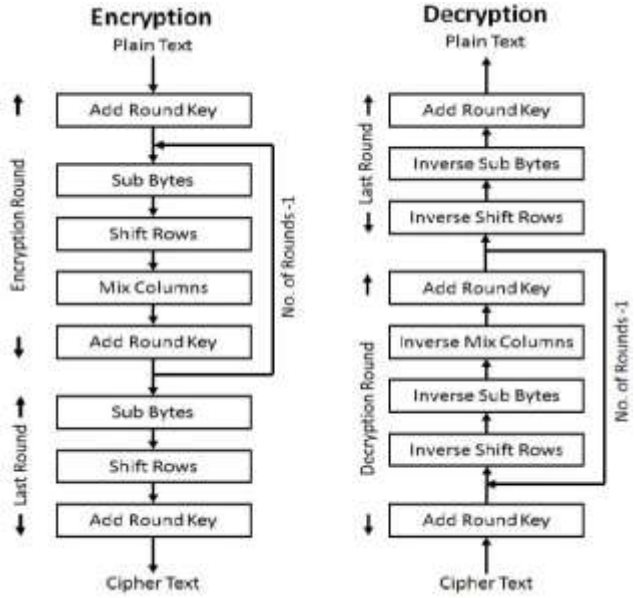

Fig-4: [3] AES ALGORITHM BLOCK DIAGRAM

B. Elliptic Curve Digital Signature Algorithm (ECDSA)

[1] The ECDSA algorithm produces the digital signature using Elliptic Curve. Hence, it is known as Elliptic Curve Digital Signature algorithm. Whereas the key size in ECDSA is smaller, but the security is achieved at a greater level. Both the Sender and Receiver should mutually accept an Elliptic curve (pr,b, c,Gen,nu,i) with the parameters. The Sender picks two keys namely: private (PRsend) and public key (PUsend). The two keys are appropriate for ECC (Elliptic Curve Cryptography). The generated keys can be used to create and verify the Digital Signature.

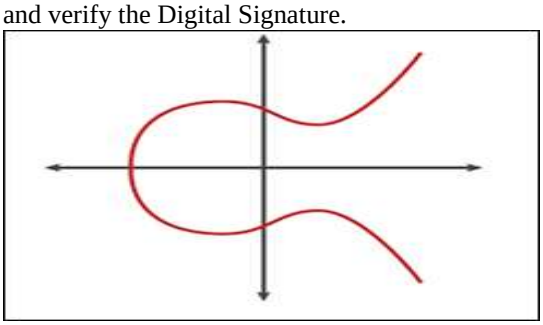

Fig -5: [1] Elliptic curve equation $z^2=y^3+by+c$

PARAMETERS	EXPLANATION
pr	Prime no. defines the field over the curve
Gen	Generator Point
b,c	Coordinates on the Elliptic Curve equation
nu	Prime factor of Gen
i	Co-factor

Table 2: Elliptic Curve Parameters

SENDER(SIGNING)	***RECEIVER(VERIFICATION)***
• Compute f=H(msg) • Choose a secret random integer 'ke' • keGeg=(p1,p2) • ver=p1 mod nu. Check whether ver=0, then move to step 2. • sign=ke $^{-1}$(f+PR$_{send}$ ver) mod nu. Move to step 2, if sign=0. • Signature = (ver,sign)	• Compute f=H(msg) • x=sign^{-1}(mod) nu. • z1=fx mod nu and z2=ver x mod nu. • (p1,p2)=z1 + z2 PU$_{send}$ The Signature is correct only if p1=ver mod nu. If not, invalid.

Table 3: Elliptic Curve Digital Signature Algorithm

IV. RESEARCH

As the data need to be transmitted securely over the network, spoofing and sniffing need to be disallowed from the attackers. The proposed algorithm keep the MAC address confidential by using AES key. Then the signature is authenticated with ECDSA algorithm. Thus, the network traffic sniffing by the hackers are not permitted.

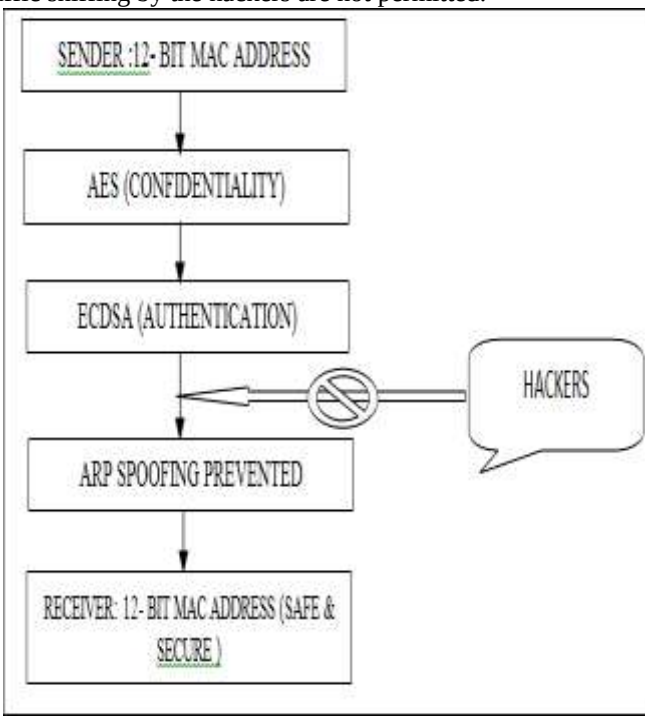

Fig-6: BLOCK DIAGRAM OF THE PROPOSED ALGORITHM

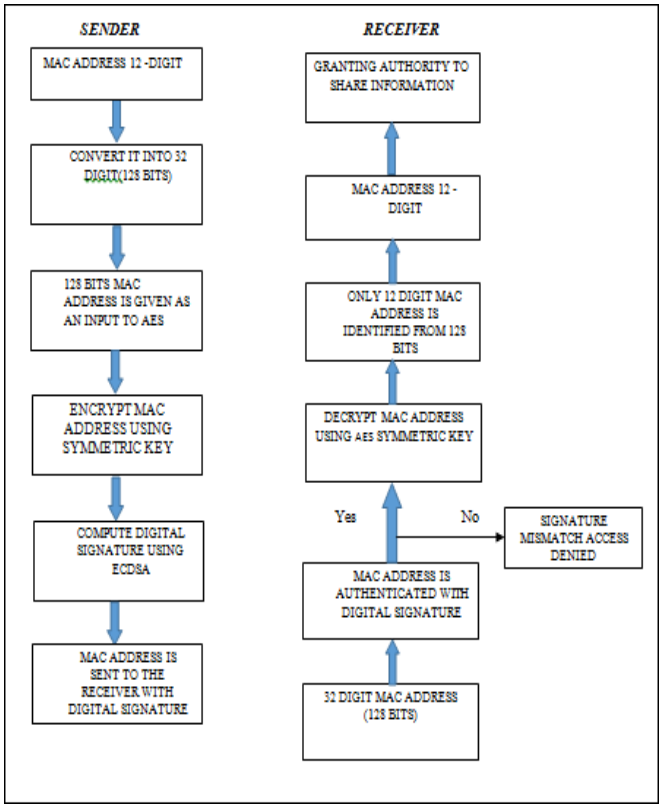

Fig -7: FLOW CHART REPRESENTATION OF THE PROPOSED ALGORITHM

V. IMPLEMENTATION AND RESULTS

The proposed algorithm is implemented in Python script for data security. The python dependencies such as pycrypto, ecdsa etc…need to be installed to run this code.

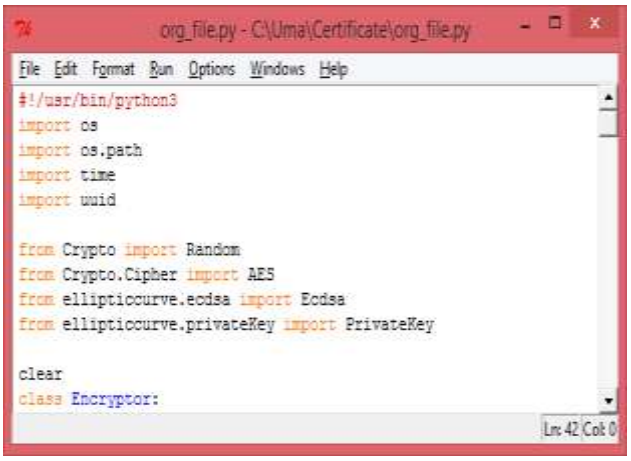

Fig- 8: Proposed algorithm implemented in Python

Fig-9: python version

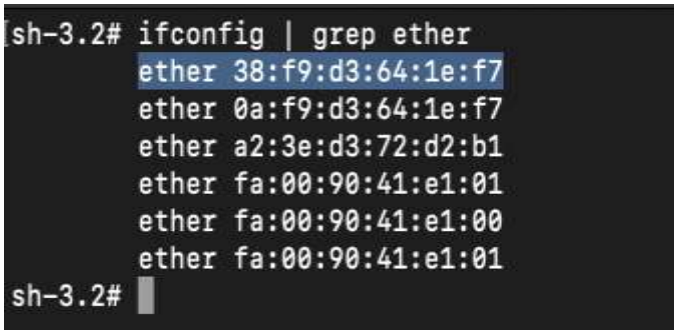

Fig -10: MAC Addresses

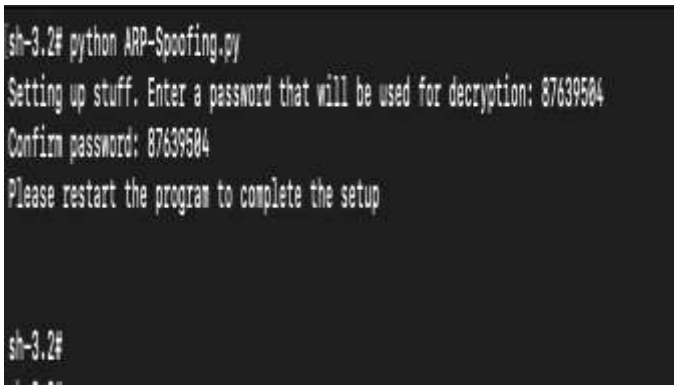

Fig -11:Sender

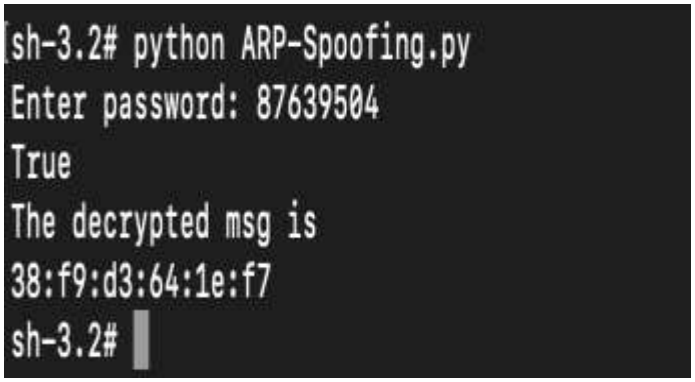

Fig -12: Receiver

VI. CONCLUSION

During the data communication for the IOT devices over the network, the data as well as the device need to be kept confidential and authenticated by the receiver. For this, Cryptographic algorithms are highly used to prevent from various attacks by the hackers. The hybrid implementation of AES and ECDSA algorithm provides the harmless and protected channel for communicating between the devices. The Man –in –the-middle, Denial-of- Service and ARP spoofing attacks are prohibited in the proposed algorithm. The MAC address plays a vital role in the algorithm. The MAC address is encrypted and decrypted by using AES and verified with the digital signature by ECDSA. Thus the hackers couldn't predict the MAC address of the sender and hence the ARP spoofing attack is prevented.

REFERENCES

1. V.K.Pachghare , "Cryptography and Information Security",PHI Learning Private Limited 2009.
2. William Stallings, "Cryptography and Network Security", Prentice Hall of India,2008.
3. https://www.semanticscholar.org/paper/A-new-dynamic-secured-IEEE-802.11e-AES-basedsystemMamdouhSadek/e46071c7eb742bcd9798ddb29ff04db1163cd121/figure/1
4. 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.
5. 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.
6. 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.
7. 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.

8. Deepika Khambra,Poonam Dabas, " Secure Data Transmission using AES in IOT", International Journal of Application or Innovation in Engineering & Management(IJAIEM), ISSN: 2319-4847, Vol. 6,Issue 6, June 2017.
9. KrishnaKanth Gupta, Sapna Shukla, "Internet of Things: Security Challenges for Next Generation Networks", 2016 1st International Conference on Innovation and Challenges in Cyber Security(ICICCS 2016), IEEE.
10. 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.
11. Ravula Arun Kumar, Kambalapally Vinuthna, "A Review on various secure data access and techniques in Fog for Internet Of Things", International Journal of Computer Sciences and Engineering(IJCSE), E-ISSN: 2347-2693, Vol.6, Issue 1,2018.
12. Pengfei Hu et al., "Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things", 2016 IEEE Internet of Things Journal.
13. Nadeem Abbas, "A Mechanism for Securing IOT –enabled Applications at the Fog layer", Journal of Sensor and Actuator Networks, 2019.
14. Deepika Khambra,Poonam Dabas, " Internet Of Things: A perspective from Security and privacy", International Journal of Advanced Research in Computer Science , ISSN: 0976-5697, Vol. 8,Issue 5, June 2017.
15. 15. Nuzhat Khan et al., "Performance Analysis of Security Algorithms for IOT devices", 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 21-23 Dec 2017, Dhaka, Bangladesh.
16. 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.
17. Ritambhara, Alka Gupta, Manjit Jaiswal, "An Enhanced AES algorithm Using Cascading Method on 400 Bits Key Size Used in Enhancing The Safety Of Next Generation Internet Of Things(IOT), ICCCA 2017,IEEE.
18. 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.