International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-3
International Conference on Research and Recent Trends in Engineering and Technology. (ICRRTET)
Held on 27th January 2016 organized by **Sai Polytechnic College,** Kinhi Jawade, Yavatmal, Maharastra, India.

Securing Domain Name System Using Advanced Encryption Standard

Miss. Priya S.Trivedi; Miss. Rupal R. Tamboli & Prof. P.M.Gourshettiwar

ABSTRACT:

The mapping of IP addresses to host names is a major problem in rapidly growing internet. The higher level binding effort went on increasing to different level of development up to the currently used Domain Name System. DNS, being an open source, it is less secured and it has no means of determining whether domain name data come from an authorized domain owner. So these vulnerabilities lead to a number of attacks. Hence, there is a need of securing DNS. This paper approaches the Advanced Encryption Standards that uses symmetric key concepts. Domain Name System has number of workgroups and these workgroups are connected to the server. This server is connected to the server of other domain and the proposed system secures client that is attacked, using AES.

***Index Terms*:** DNS Security, Public Key infrastructure, AES

INTRODUCTION

DNS is a client server application that maps host names into their corresponding IP address. The DNS is internet directory service. It is considered as one of the most important components of the modern internet. A domain name is a meaningful and easy-to-remember handle for IP address. There are various types of attacks which can be occurred on DNS. One type of attack is black hole attack. This black hole attack can be prevented by using AES algorithm. An advanced encryption standard algorithm (AES) is a symmetric key block cipher; here same key is used for both encryption and decryption. Its key size is variable depending on the number of rounds; it can be 128,192 or 256. Because of large key size it provides more security. It is resistant against all known attacks and it is easy to implement. The AES encryption algorithm is a block cipher that uses an encryption key and a several rounds of encryption. A block cipher is an encryption algorithm that works on a single block of data at a time. In the case of standard AES encryption the block is 128 bits, or 16 bytes, in length. The term "rounds" refers to the way in which the encryption algorithm mixes the data re-encrypting it ten to fourteen times depending on the length of the key. A number of people have created source code implementations of AES encryption, including the original authors. In this proposed system we are using NS2 as a implementation tool because it gives good simulation as compared to other tools. [3]

AES have mainly three advantages. These include having large key size, providing more security and its design simplicity. As securing is the most important part of Domain Name System, it is better to consider AES as the main tool for its implementation.

Advanced Encryption Standard, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES encrypt the data blocks of 128 bits in 10, 12 and 14 round depending on the key

size. Black Hole attack is the only effective attack known against this algorithm. AES encryption is fast and flexible. [2]

Advanced Encryption Standard is algorithm which uses only one key for encrypting and decrypting the data. Both user that is sender and receiver shares the same key.The keys may be identical or there may be simple transformation to go between the two keys.

For encryption, each round consists of the following four steps:

1) Substitute bytes,
2) Shift rows,
3) Mix columns, and
4) Add Round key

The last step consists of XORing the output of the first three steps and for decryption, each round consists of the following four steps:

1) Inverse shift rows,
2) Inverse substitute bytes,
3) Add round key, and
4) Inverse mix columns. The third step consists of XORing the output of the first two steps.

IMPLEMENTATION OF AES

AES consist of 4 different stages sown below:

- Add Round Key.
- Substitute Bytes
- Shift Rows
- Mix column

1.Add Round key:

Add round key stage is a simple bitwise XOR of a current block with a portion of expanded key. This step makes use of key. It must be used at start and end of each round. The number of rounds for each bytes are fixed.

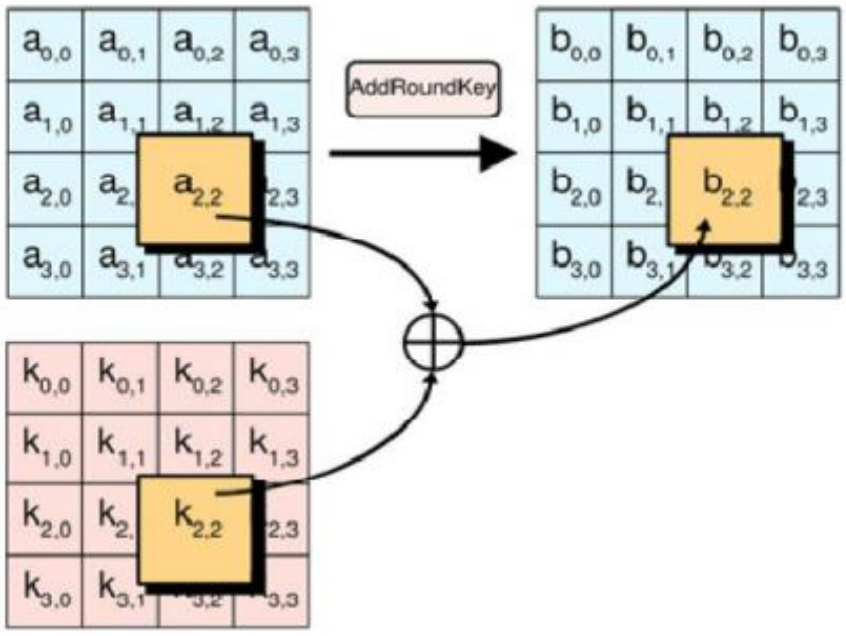


Fig. 3.1.1 Add Round key

2. Substitute Bytes:

i. Each byte of state is replaced by byte indexed by row (left 4-bits) & column (right 4-bits).

ii. S-box constructed using defined transformation of values in GF (2^8).

EA	04	65	85	→	87	F2	4D	97
83	45	5D	96		EC	6E	4C	90
5C	33	98	B0		4A	C3	46	E7
F0	2D	AD	C5		8C	D8	95	A6

Fig. 3.1.2. Substitute Bytes

3.Shift Rows:

Arrange the states in a matrix and then perform the circular shift for each row. This is not a bitwise shift. The circular shift just moves each byte one space over.

- 1st row is unchanged.
- 2nd row does 1 byte circular shift to left.
- 3rd row does 2 byte circular shift to left.
- 4th row does 3 byte circular shift to left.
- Decrypt inverts using shifts to right.
- Since state is processed by columns, this step permutes bytes between the columns.

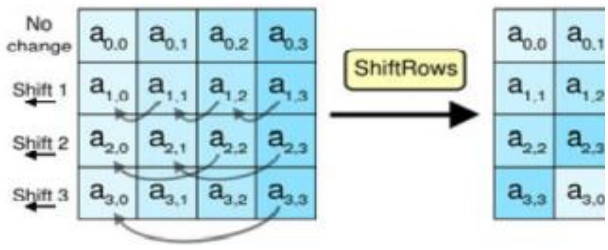


Fig. 3.1.3 Shift Row

4.Mix columns:

There are two parts to this step. The first will explain which parts of the state are multiplied against which parts of matrix. The second will explain how this multiplication is implemented.

- The state is arranged into a 4 row table.
- Each column is processed separately.
- Each byte is replaced by a value dependent on all 4 bytes in the column.
- For decryption it requires uses.

87	F2	4D	97	→	47	40	A3	4C
6E	4C	90	EC		37	D4	70	9F
46	E7	4A	C3		94	E4	3A	42
A6	8C	D8	95		ED	A5	A6	BC

Fig.3.1.4 Mix column

({02} • {87}) ⊕ ({03} • {6E }) ⊕ {46} ⊕ {A6} = {47}

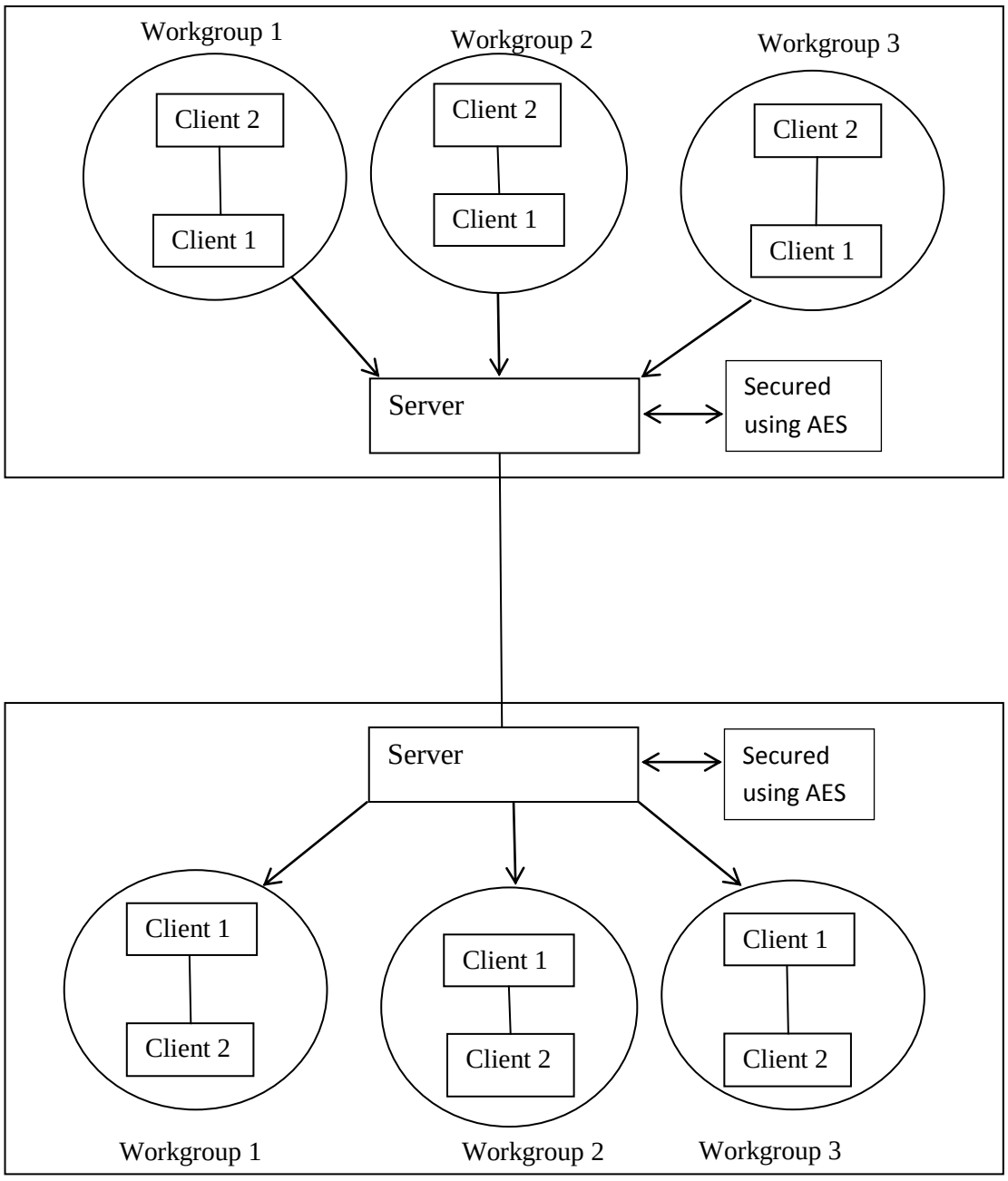
{87} ⊕ ({02} • {6E }) ⊕ ({03} • {46}) ⊕ {A6} = {37}

{87} ⊕ {6E } ⊕ ({02} • {46}) ⊕ ({03} • { A6}) = {94}

({03} • {87}) ⊕ {6E } ⊕ {46} ⊕ ({02} • { A6}) = {ED}

Fig .3.1.4 Example Mix Column

SYSTEM ARCHITECTURE



MODULES DESCRIPTION

These paper approaches to AES algorithm. AES is a symmetric block cipher i.e., it uses a single key for encryption and decryption that makes it more securable. It is easy to implement as compared to other algorithms. Implementation of this proposed system includes three different modules.

1) Client module-

The workgroup of different domains holds different clients. These clients communicate within themselves in the same domain and also with the other clients that are present in other domain. This leads to the black hole attack if any unauthorized message is forwarded. Thus the attack occurs on the client and not on the server. This client is thus prevented using AES algorithm which is implemented on the server. There can be any number of clients present in the workgroup.

2) Server module-

It is the most essential module of the proposed system. Server connects the various clients of their respective domains. When attack occurs on any of the client of the domain, it is prevented using AES. This AES is implemented on the server. The work of server is to detect whether the sender is authorized one or not if it is authorized it will continue sending the message but if not, then it will detect their attack occurred i.e., black hole attack. And thus it is prevented using AES. AES is implemented on both the server of both domains.

3) Domain module-

The domain of the system combines together the clients and the server. It mainly consists of workgroups. These workgroup holds the clients. These workgroups are connected to the server. The two domains are thus connected to each other by the connecting media further that connects the two main servers of different domain.

CONCLUSION

This paper propose the implementation of Encryption and decryption for AES algorithm. We implement different sub modules for AES algorithm . This implementation will be useful in the domain name system to prevent it from the attack. Encryption is successfully completed by the use of key expansion and transformations of shift Rows, sub bytes, mix columns, add round keys. The AES algorithm can be efficiently implemented by software (NS2). NS version 2 implementations cost the smallest resources, but they offer a limited physical security and the slowest process. Besides, growing requirements for high speed, high volume secure communications combined with physical security, hardware implementation of cryptography takes place.

REFERENCES

[1] Xinmiao Zhang and Keshab K. Parhi "Implementation Approaches for the Advanced Encryption Standard Algorithm" IEEE 2002

[2] X. Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm,"IEEE Transactions on Very Large Scale Integration Systems,vol.12, issue 9, pp.95 967, Sep. 2004.

[3] Hui QIN, Tsutomu SASAO, Yukihiro IGUCHI "An FPGA Design of AES Encryption Circuit with 128-bit Keys"GLSVLSI'05, ACM 2005.

[4] Sachin Kumar Sinha, Avinash Kant Singh, Amaresh Sharma "Security System for

DNS using Cryptography" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 2, February-2013.

[5] PallaviAtha et al, "Design & Implementation Of AES Algorithm Over FPGA Using VHDL", International Journal of Engineering, Business and Enterprise Applications (IJEBEA)", ISSN (Online): 2279-0039,pp. 58-62,2013.