Securing Data Encryption

Dr. Kiramat ullah, Abbas Khurum, Zeeshan Haider
Pakistan Institute of Engineering and Applied Sciences (PIEAS)
ARID Agriculture University.

Abstract: This article provide analysis about information security using cryptography techniques. After the analyzing different techniques of encryption, we are proposing Advance Encryption Standard (AES). The AES has the better security compared others encryption algorithm and prevent data from Spoofing. It is very efficient in both hardware and software.

Keywords: **Encryption, Security, Cryptography, Encoding.**

I. Introduction

Data Encryption is the process of converting the plaintext into Encoded form (non-readable) and only authorized person/parties can access it. Data security is an essential part of an Individual/organization; it can be achieved by the using various methods. The encrypted data is safe for some time but never think it is permanently safe. After the time goes on there is chance of hacking the data by the hacker. Fake files are transmitted in the same manner as one can sends the encrypted data. There are many algorithms available in the market for encrypting the data. Encryption Key has the major role in the overall process of data.

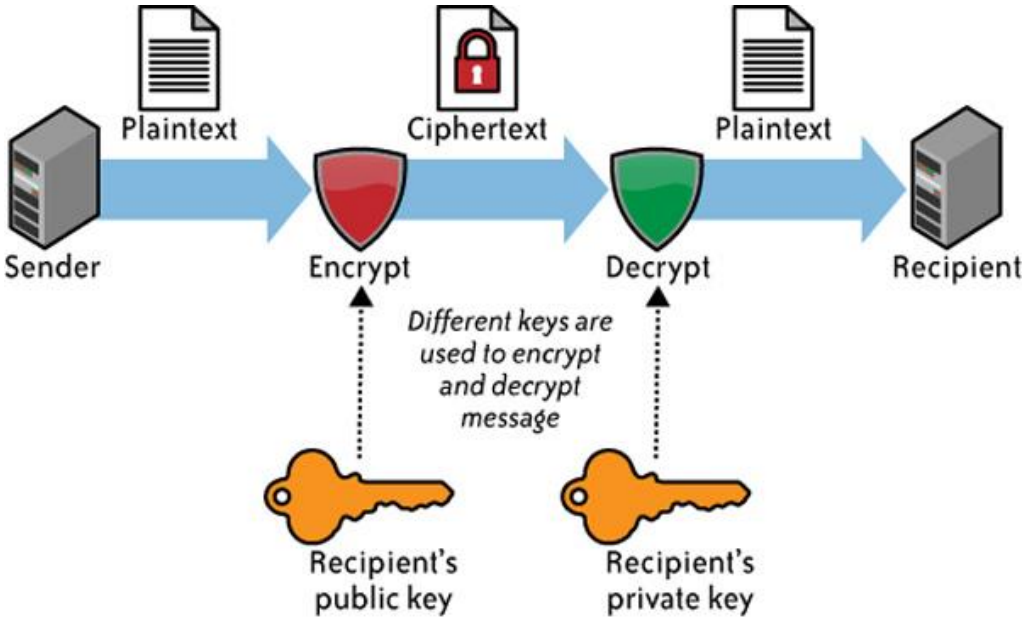

Fig1 Encryption and Decryption process

II. Methodology

In this article, we have considered Various Encryption Algorithms and Techniques for improving securing data, Information Security using encryption. Comparisons of encryption algorithms on the basis of their performance, key size, efficiency in hardware and software, availability, implementation techniques, and speed.

III. Results

3.1 Summary of algorithms

We compare measured speed of encryption with various algorithms available as standard in Oracle JDK, using Eclipse IDE and then give a summary of various other characteristics of those algorithms. The encryption algorithms is consider here are AES (with 128 and 256-bit keys), DES, Triple DES, IDEA and Blowfish (with a 256-bit key).

3.2 Performance

First, the easy bit. Figure 4 shows the time taken to encrypt various numbers of 16-byte blocks of data using the algorithms mentioned.

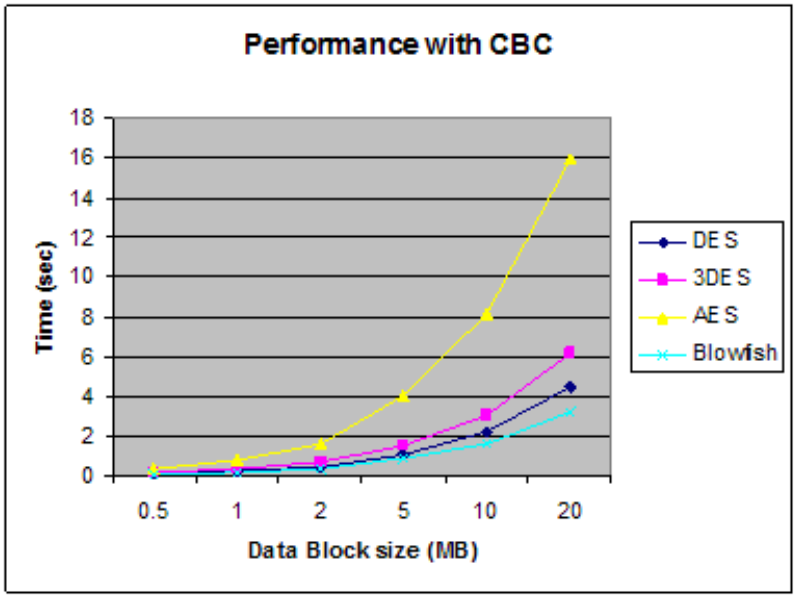

Fig4 Comparison of encryption times for various common symmetric encryption algorithms [1]

It's important to note right from the beginning that beyond some ridiculous point, it's not worth sacrificing speed for security. However, the measurements will still help us make certain decisions.

3.3 Characteristics

Table 1: gives a summary of the main features of each encryption algorithm, with what I believe is a fair overview of the algorithm's current security status.

Factors	RSA	DES	3DES	AES
Created By	Ron Rivest, Adi Shamir, and Leonard Adleman In 1978	IBM in 1975	IBM IN 1978	Vincent Rijmen, Joan Daemen in 2001
Key Length	Depends on number of bits in the modulus n where n=p*q	56 bits	168 bits (k1, k2 and k3) 112 bits (k1 and k2)	128, 192, or 256 bits
Round(s)	1	16	48	10 - 128 bit key,12 - 192 bit key,14 - 256 bit key
Block Size	Variable	64 bits	64 bits	128 bits
Cipher Type	Asymmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Speed	Slowest	Slow	Very Slow	Fast
Security	Least Secure	Not Secure Enough	Adequate Security	Excellent Security

Table 1: Characteristics of commonly used encryption algorithms

IV. Discussion

Some important encryption algorithms are discussed here:

4.1 Data Encryption Standard (DES)

It is one of the most widely accepted, publicly available cryptographic systems today. It was developed by IBM in the 1970s but was later adopted by the US government as a national bureau of standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976. It uses a 56-bit key to encrypt the 64 bit block size data. It processes 64-bit inputs into 64-bit cipher-text and algorithm performs 16 iterations.

4.2 International Data Encryption Algorithm (IDEA)

IDEA is a block cipher designed by James Massey and Xuejia Lai and was first described in 1991. It uses 128 bit key length which operates on 64 bit blocks. It consists of a series of eight identical transformations based upon bitwise exclusive-or, addition and multiplication modules. It is based upon symmetric cipher and has very weak key design method therefore security level of the algorithm is very poor as compared to the DES. IDEA not becomes so much popular due to its complex structure.

4.3 Blowfish

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention.

4.4 Triple DES (TDES)

It was developed in 1998 and derived from DES. It applies the DES cipher algorithm three times to each of the data blocks. Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three keying options in data encryption standards:
All keys being independent Key 1 and key 2 being independent keys All three keys being identical
Key option #3 is known as triple DES. The triple DES key length contains 168 bits but the key security falls to 112 bits.

4.5 Twofish

It was derived from blowfish by Bruce Schneier in 1998. It is freely available in the public domain as it has not been patented. It is a symmetric key block cipher having key sizes 128,192 and 256 bits used to encrypt the 128 bit block size data in 16 rounds. The algorithm making use of S- Boxes and makes the key generation process very complex and secured.

4.6 Advanced Encryption Standard (AES)

It is a symmetric 128-bitblock data encryption technique developed by Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected the algorithm, called Rijndael (pronounced Rhine Dahl or Rain Doll), out of a group of five algorithms under consideration, including one called MARS from a large research team at IBM.

While the terms AES and Rijndael are used interchangeably, there are some differences between the two. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits.
It provides following services:

- It is a politically safe decision: the encryption standard of the US National Institute of Standards and Technology (NIST), and the US government reportedly approves AES with 192 or 256-bit keys for encrypting top secret documents.
- Nobody yet has (publicly) a full attack on AES, or a partial attack that is practical (though some impractical partial attacks exist5).
- AES is algebraically simpler than other block ciphers: effectively, it can be written as a series of mathematical equations.
- The NSA may have chosen Rijndael as they secretly know how to break it, or secretly estimated that they could develop a way to break it.

IV. Comparison

The techniques have been compared on the basis of that how much:

- CPU processing speed for encrypting and decrypting data.
- Speed to generate the key.
- Key size.
- Security consideration.
- Efficient on the hardware and software in case of implementation.
- The amount of memory required to hold the data in encryption process.
- Number of users accommodated by the model.
- Time required by the model to recover the data in case of key failure.
- Time available to the hacker to produce various types of attacks.
- Complexity of algorithm technique.

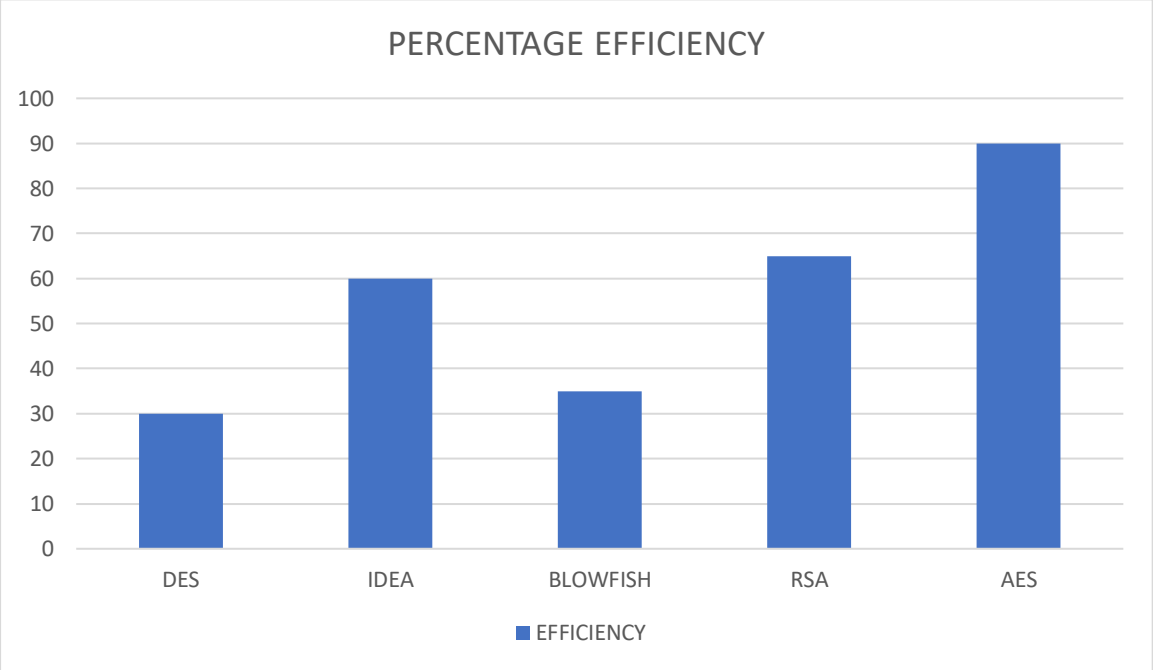

Fig5 Comparison of Encryption on the basis of Percentage Efficiency [1]

V. Formulation and Case study

5.1 Case Study

Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

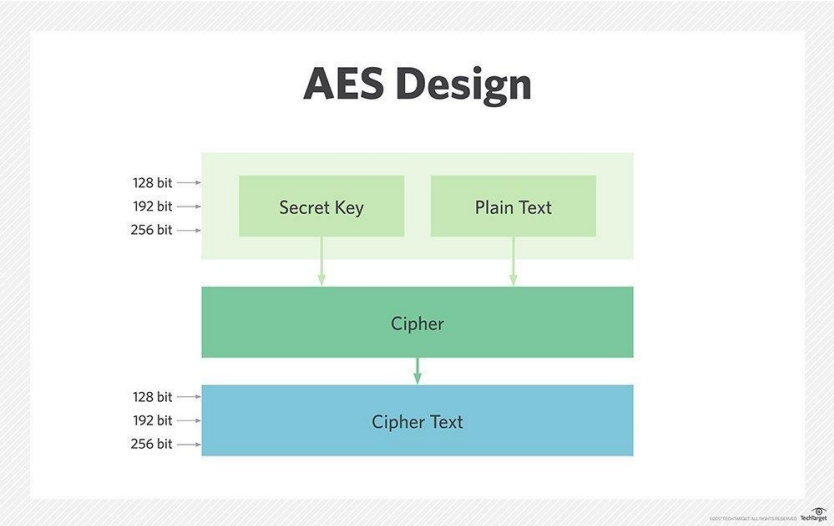

Fig6 AES Encryption conversion process

5.2 Rounds

During the encryption process of a message, if the message is not divisible by the block length, then the Padding is used. Padding is the method of adding additional Dummy data. E.g. if the message consists of 426 bytes, then we need 7 additional bytes of padding to make the message 432 bytes long, because 432 is divisible by 16.
Three key sizes can be used in AES and depending on key sizes the number of rounds in AES changes. Standard key size in AES is 128 bits and no of rounds are 10. for AES encryption two sub keys are generated and in 1st round a round key is added.

No.	Key Size	No of Rounds
1.	128 bits	10
2.	192 bits	12
3.	256 bits	14

Fig7 Explain the Key Size and No of Rounds of AES

For 128 bits plain text and 128 bits key is used and 10 rounds are performed on plain text to find the cipher text. In first step, 10 round keys are generated for each round there is separate round key. But in first round an extra round key which is initial round is added to the round and then transformation is started. Transformation consists of four steps.

1. Substitute Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key

The Following figure explain all the stages of Encryption from plain text to Cipher text.

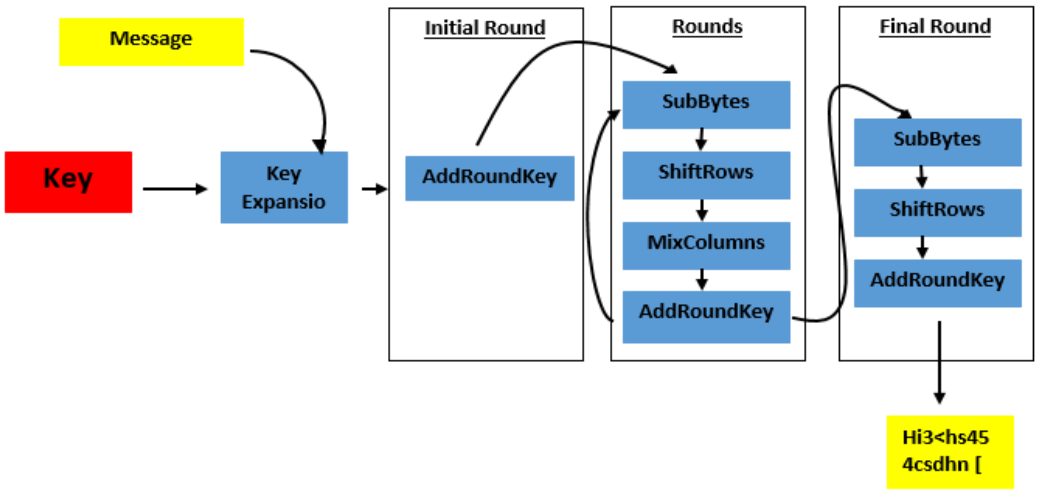

Fig8 Shows the Stages of each Round

5.3 Encryption with AES

The encryption phase of AES can be broken into three phases: the initial round, the main rounds, and the final round. All of the phases use the same sub-operations in different combinations as follows:

- **Initial Round:** **1.** Add Round Key
- **Main Round:** **1.** Sub Bytes **2.** Shift Rows **3.** Mix Columns **4.** Add Round Key
- **Final Round:** **1.** Sub Bytes **2.** Shift Rows **3.** Add Round Key

The four sub-operations of AES are AddRoundKey, SubBytes, ShiftRows, and MixColumns. These are explained in more detail in the following subsections.

5.3.1 AddRoundKey:

The AddRoundKey operation is the only phase of AES encryption that directly operates on the AES round key. In this operation, the input to the round is exclusive-ored with the round key.

5.3.2 SubBytes:

The SubBytes phase of AES involves splitting the input into bytes and passing each through a Substitution Box or S-Box. Unlike DES, AES uses the same S-Box for all bytes. The AES S-Box implements inverse multiplication in Galois Field 2^8.

5.3.3 ShiftRows:

In the ShiftRows phase of AES, each row of the 128-bit internal state of the cipher is shifted. The rows in this stage refer to the standard representation of the internal state in AES, which is a 4x4 matrix where each cell contains a byte. Bytes of the internal state are placed in the matrix across rows from left to right and down columns.

5.3.4 MixColumns:

Like the ShiftRows phase of AES, the MixColumns phase provides diffusion by mixing the input around. Unlike ShiftRows, MixColumns performs operations splitting the matrix by columns instead of rows.
Unlike standard matrix multiplication, MixColumns performs matrix multiplication as per Galois Field 2^8.

5.4 Decryption in AES:

To decrypt an AES-encrypted ciphertext, it is necessary to undo each stage of the encryption operation in the reverse order in which they were applied. The three stage of decryption are as follows:

- **Inverse Final Round:** **1.** Add Round Key **2.** Shift Rows **3.** Sub Bytes
- **Inverse Main Round:** **1.** Add Round Key **2.** Mix Columns **3.** Shift Rows **4.** Sub Bytes
- **Inverse Initial Round:** **1.** Add Round Key

VI. Improvements

There has always been a tradeoff between two things. In case of cryptographic algorithms the tradeoff is between speed and security. If we talk about speed and compromise on security then in this scenario Blowfish is more efficient than any other algorithm including AES but, if security matters to us more than speed in this case AES is most efficient. Here we are more concerned about security that which algorithm makes our data most

secure so that's why we will use AES. Every technique has some weak points. The week point of AES is speed due to its complexity. Following improvements can be made in AES:

- Use some technique to improve its speed.
- Every block is always encrypted in the same way, so by adopting some other ways of encryption techniques e.g. TDES.
- It should provide some sort of execution kit to make implementation efficient on software.
- The strength of the AES algorithm may enhance by increasing the key length from 128 bits to 512 bits and thereby the number of rounds is increased in order to provide a stronger encryption method for secure communication.

VII. Conclusion

The study of various algorithms shows that the strength of model depends upon the key management, type of cryptography, number of keys, number of bits used in a key. All the keys are based upon the mathematical properties. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data. AES data encryption is a more mathematically efficient and elegant cryptographic algorithm, but its main strength rests in the option for various key lengths. AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially strong. AES uses permutation-substitution, which involves a series of substitution and permutation steps to create the encrypted block.

References

[1] Z. Haider, M. Saleem, and T. Jamal, "Analysis of Interference in Wireless", in Proc. of ArXiv, arXiv:1810.13164 [cs.NI], Oct. 2018.

[2] T. Jamal and P. Mendes, "Relay Selection Approaches for Wireless Cooperative Networks", in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.

[3] T. Jamal, P. Mendes, and A. Zúquete, "Opportunistic Relay Selection for Wireless Cooperative Network", in Proc. of IEEE IFIP NTMS, Istanbul Turkey, May 2012.

[4] T. Jamal and P. Mendes, "Cooperative relaying in user-centric networking under interference conditions", in Proc. of IEEE Communications Magazine, vol. 52, no. 12, pp. 18–24, Dec 2014.

[5] P. Mendes, W. Moreira, T. Jamal, and Huiling Zhu, "Cooperative Networking in User-Centric Wireless Networks", In: Aldini A., Bogliolo A. (eds) User-Centric Networking. Lecture Notes in Social Networks. Springer, Cham, ISBN 978-3-319- 05217-5, May 2014.

[6] T. Jamal, P. Mendes, and A. Zúquete, "Relayspot: A Framework for Opportunistic Cooperative Relaying", in Proc. of IARIA ACCESS, Luxembourg, June 2011.

[7] T. Jamal, and SA Butt, "Malicious Node Analysis in MANETS", in Proc. of International Journal of Information Technology, PP. 1-9, Springer Publisher, Apr. 2018.

[8] T. Jamal, and P. Mendes, "COOPERATIVE RELAYING FOR DYNAMIC NETWORKS", EU PATENT, (EP13182366.8), Aug. 2013.

[9] T. Jamal, and P. Mendes, "802.11 Medium Access Control In MiXiM", in Proc. of Tech Rep. SITILabs-TR-13- 02, University Lusófona, Lisbon Portugal, Mar. 2013.

[10] T Jamal, M Alam, and MM Umair, "Detection and Prevention Against RTS Attacks in Wireless LANs", in Proc. of IEEE C-CODE, Islamabad Pakistan, Mar. 2017.

[11] L. Lopes, T. Jamal, and P. Mendes, "Towards Implementing Cooperative Relaying", In Proc. of Technical Report COPE-TR-13-06, CopeLabs University Lusofona Portugal, Jan 2013.

[12] T. Jamal, P. Mendes, and A. Zúquete, "Interference-Aware Opportunistic Relay Selection", In Proc. of ACM CoNEXT student workshop, Tokyo, Japan, Dec. 2011.

[13] T. Jamal, "Cooperative MAC for Wireless Network", In Proc. of 1st MAP Tele Workshop, Porto, Portugal, 2010.

[14] T. Jamal and P. Mendes, "Analysis of Hybrid Relaying in Cooperative WLAN", In Proc. of IEEE IFIP Wireless Days (WD), Valencia, Spain, November 2013.

[15] T. Jamal, and P. Mendes, "Cooperative Relaying for Wireless Local Area Networks", In: Ganchev I., Curado M., Kassler A. (eds) Wireless Networking for Moving Objects. Lecture Notes in Computer Science, vol 8611. Springer, Cham, (WiNeMo), Aug. 2014.

[16] T. Jamal, and SA Butt, “Cooperative Cloudlet for Pervasive Networks”, in Proc. of Asia Pacific Journal of Multidisciplinary Research, Vol. 5, No. 3, PP. 42-26, Aug 2017.

[17] T. Jamal, P. Mendes, and A. Zúquete, “Wireless Cooperative Relaying Based on Opportunistic Relay Selection”, in Proc. of International Journal on Advances in Networks and Services, Vol. 5, No. 2, PP. 116-127, Jun. 2012.

[18] SA Butt, and T. Jamal, “Frequent Change Request from User to Handle Cost on Project in Agile Model”, in Proc. of Asia Pacific Journal of Multidisciplinary Research 5 (2), 26-42, 2017.

[19] T. Jamal, and P. Amaral, “Flow Table Congestion in Software Defined Networks”, in Proc. of IARIA 12th ICDS, Rome Italy, Mar. 2018.

[20] R. Sofia, P. Mendes, W. Moreira, A. Ribeiro, S. Queiroz, A. Junior, T. Jamal, N. Chama, and L. Carvalho, “Upns: User Provided Networks, technical report: LivingExamples, Challenges, Advantages”, Tech. Rep. SITI-TR- 11- 03, Research Unit in Informatics Systems and Technologies (SITI), University Lusofona, Lisbon Portugal, Mar. 2011.

[21] T. Jamal, and P. Mendes, “Cooperative Relaying in Wireless User-Centric Networks”, Book Chapter In: Aldini, A., Bogliolo, A. (eds.) User Centric Networking. Lecture Notes in Social Networks, Springer, Cham, pp. 171–195, 2014.

[22] T. Jamal, P. Mendes, and A. Zúquete, “Design and Performance of Wireless Cooperative Relaying”, PhD Thesis MAP-Tele, University of Aveiro, Oct. 2013.

[23] T. Jamal, P. Mendes, and A. Zuquete, “RelaySpot: Cooperative Wireless Relaying”, in Proc. of MAP-Tele Workshop, Aveiro, Portugal, May 2011.

[24] T. Jamal, and P. Mendes, “Cooperative Wireless Relaying, Key Factors for Relay Selection”, in Proc. of MAP- Tele Workshop, Porto, Portugal, Dec. 2009.

[25] SA Butt, and T. Jamal, “Study of Black Hole Attack in AODV”, in Proc. of International Journal of Future Generation Communication and Networking, Vol. 10, No.9, pp. 37-48, 2017.

[26] T. Jamal, and SA Butt, “Low-Energy Adaptive Clustering Hierarchy (LEACH) Enhancement for Military Security Operations”, In Proc. Of Journal of Basic and Applied Scientific Research, ISSN 2090-4304, 2017.

[27] T. Jamal, and P. Mendes, “RelaySpot, OMNET++ Module”, Software Simulator Extension In Proc. of COPE- SW-13-05, 2013.

[28] T. Jamal and Z. Haider, "Denial of Service Attack in Cooperative Networks", in Proc. of ArXiv, arXiv: CoRR Vol. arXiv:1810.11070 [cs.NI], Oct. 2018.

[29] Zeeshan Haider, Kiramat Ullah and T. Jamal, "DoS Attacks at Cooperative MAC", in Proc. of ArXiv, arXiv:1812.04935 [cs.NI], Dec. 2018.