*Sindh Univ. Res. Jour. (Sci. Ser.) Vol. 51 (2) 291-294 (2019)*

http://doi.org/10.26692/sujo/2019.6.48

**SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)**

# Network Security Using Python: An Empirical Analysis of Advance Encryption Standard (AES)

A. BURDI, A. A. KHAN*, S. AWAN*, F. A. ABBASI**, S. H. F. NAQVI, A. R. NIZAMANI

Institute of Mathematics & Computer Science: University of Sindh, Jamshoro

Received 5th January 2019 and Revised 12thMay 2019

**Abstract:** Nowadays, security in network environment is becoming a challenging problem, providing prevention of confidential records arises as a critical task. Modern creation in network can reduce the rate of uncertainty as-well-as at the same time growth of threats increases rapidly in past few decades i.e. vulnerabilities, and potential risks. Confidentiality of crucial informationis one of the main objectives, to protect integrity when its traveling from one node to another, ensure it can't divulge by malicious insider, anonymous, trust, and malicious attacks.In this research paper, the proposed solution is to design interface where communication can be done in a secure manner, behind it has a mechanism which hide essential information, symmetric key cryptographic algorithm named advance encryption standard (AES) using python with additional library called pycrypto and tries to formulate algorithm efficiency, accuracy, execution time plus system capability.

**Keyword:** Empirical Analysis, Advance Encryption Standard (AES), Threads, Encryption & Decryption, Python.

## 1. INTRODUCTION

In (1969), Advanced Research Project Agency (ARPA) interconnected four universities' computer systems for sharing crucial resources related to scientific key points under the direction of U.S. After couple of years, the word internet arising as a network of network, which aim to provide communication between nodes, share information without hinderances. At the same time threats involve which harm integrity of confidential information.

The main motive is to design secure path and make communication deliverable as well as realiable. Considering prevention of the information from different types of threats. There are several examples of attacks arises in past few decades; malware is one of the main examples of threat where malicious software can harm computer devices, such as worms, viruses, trojan horses, spyware and others. Ransom ware restricted user to access the computer system or files and display message that demands payment in order to removed restriction. Pharming is an online fraud, redirecting users to the fake sites (even you entered the correct URL), illegitimate website can convince user that its real (legitimate)site and ask personal information or other details. Hacking is someone to gain unauthorized access (without getting permission) to run computer. Find weaknesses in security settings then enter in the system and misuse your information. Spoofing is the technique which steal information just like phishing. The below section describes some critical problems available in network environment.

The word crypto contributes lots of mechanisms which change the perspective of communication with a secure manner. Multiple algorithms of cryptography are running for providing prevention from unknown sources, used as a data protection and ensure it will deliver as the authorized user. Recently, all those security algorithms were cracked except Advanced Encryption Standard (AES). AES algorithm plays a vital role to resolve critical problem of reliable communication between authorized people. The next section elaborates cryptographic algorithms related literatures regarding objectives, importance, and features.

## 2. RELATED LITERATURE

In this context, reviewing some effective literatures related to cryptographic algorithm AES capability, accuracy, and efficiency using different programming languages. Most of the scholars wrote critical challenges arise in past couples of years regarding data confidentiality, integrity, availability & control access. The priority set to provide security, when data is traveling from one to another node. Dakhare Bhawana et.al describes the importance of AES, Blowfish, SNAP algorithms and compare the experimental results. The main objective is to check performance, file size, time required to upload the file on cloud. SNAP provides more accuracy in terms of security and takes less amount of time to upload file as compare to AES (Dakhare, 2018), contributes efforts in the field of network security, explain the importance of AES in cloud environment for the protection of electronic

Email: asad.buledi@usindh.edu.pk, abdullah.khan00763@gmail.com, shafique.awan@bbsul.edu.pk, faheem.abbasi@usindh.edu.pk, hira.naqvi@usindh.edu.pk
*Department of Computer Science Benazir Bhutto Shaheed University Lyari, Karachi
**Institute of Information and Communication Technology, University of Sindh, Jamshoro

health record of health-care sector (Arunkumar, *et al.*, 2017). uses encryption in multimedia big data of IoT. Symmetric cryptographic algorithms are used to reduce the computational cost and increase throughput especially AES and genetic algorithm (Arunkumar, 2017). .A novel hybrid encryption algorithm based on chaos. It is design for image security & effectiveness. (Çavuşoğlu, 2018) recommend AES for chaos encryption, more secure and reliable for image security (Çavuşoğlu, 2018). The comparative study of carious cryptography's algorithms. In this survey, there are four basic evaluation parameters (architecture, flexibility, security & scalability), which help to choose specific algorithm for critical situations. The main goal of data security is confidentiality, integrity, availability & authenticity (Pandey, and Verma. 2015). Compared symmetric-key cryptographic well-known algorithms named: DES, 3DES & AES. Comparison in terms of speed, time, throughput, key length, round & block size, researchers found AES is the best one (Sivakumar, *et al.*, 2018) elaborates the key importance of encryption algorithms in cloud computing. In cloud, storage-as-a-service needs more protection than others; because client's data or files are stored, in this situation, prevention can only be done by using encryption standards (Li, 2017). A comprehensive study of AES, DES, 3DES, RSA & Blowfish. highlight the critical issue generating on internet environment such as cybercrime. The parameter design to send & receive data in terms of less cost, increase performance, storage (block size), file size & time. Result shows that Blow fish takes less amount of time, but AES gives more efficiency & file storage (Patil, 2016). At last, considering AES performing outstanding in almost every programming language of data security. Now, we're going to enhance the performance as-well-as utilizing in a better manner by using Pycrypto in Python IDE.

## 3. METHODOLOGY

The proposed solution is to redesign and utilize AES for the protection of information from unauthorized access, hiding confidential information with the help of encryption (ciphertext) and decryption (plaintext).The steps indicate the overall process of AES algorithm; In first step, data should be entered in the form of alphanumeric characters, symmetric key generate by the algorithm for hiding information, ciphertext share with authorized people and it can't creak by unknown sources, decoding only be perform when providing symmetric key, if code valid then the actual message display otherwise error generate. These crucial steps elaborate the overall mechanism of encryption & decryption of AES. The secure channel without any alteration, transfer confidential information form authorized-to-authorized people **(Fig. 1).**

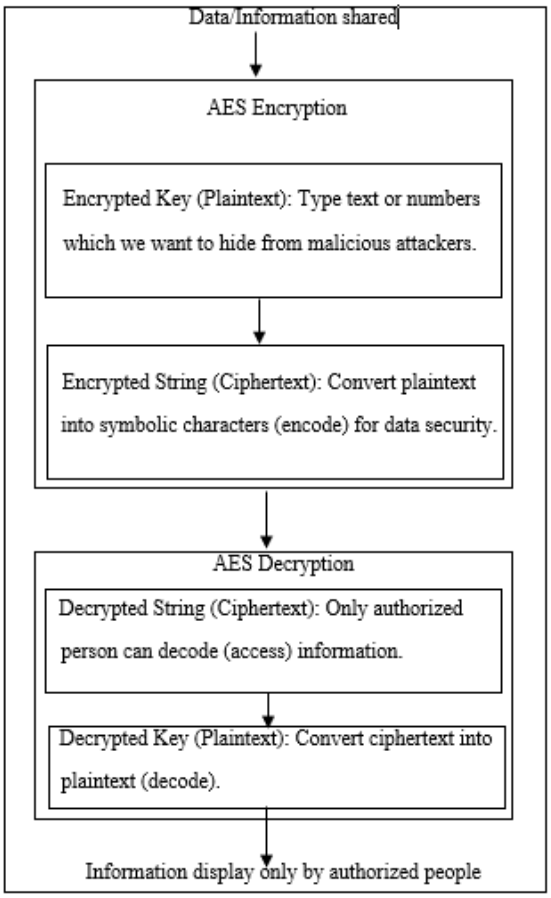


***Fig. 1 - Steps of the Propose Solution of AES***

### 3.1. System Requirement

In this research, Haier Y11C machine used to design & implement AES algorithm. The system based on RISC 64-bits architecture x64. System Specifications are mention below:

Intel(R) Core (TM) m3 7th generation,
1.00GHz 1.61GHz processor,
8 GB RAM,
1TB HDD,
Intel(R) HD Graphic Display,
and some useful peripheral devices.
The system specification helps to achieve goal in an efficient and accurate manner.

### 3.2. Software Requirement

The software specification splits into two sub parts, one is system and other is application software. Software specification describe below:

- Microsoft Windows 10 64-bits (System software)
- Python 3.6.5 (Application software)
- Miniconda 3.6

- Spyder IDE

Above mention software helps to utilize pycrypto for accessing algorithm's advanced features.

### 3.3. Advance Encryption Standard (AES)

AES is a symmetric key cryptography chosen by U.S government to secure sensitive information throughout the world[1].In 1977, NIST (National Institute of Standard & Technology) started development of AES. After the brute-force attack on DES algorithm, researchers started to create a successful Data Encryption Algorithm known as AES. Rijndael (Rijmen & Daemen) implemented AES in 2000 and published by NIST. In 2002, became federal government standard in U.S. The important features of AES are; it can handle 128-bit blocks of cipher block, it contains 128, 192 and 256 bitsof key size, resist attacks as compare to other algorithms, cost effective, flexible and more suitable to implement in any hardware & programming language. It's more powerful than DES & 3DES because stronger & longer user key length. The crucial steps of AES algorithms are; cipher put the data into an array, after cipher transformations are repeated numbers of encryption rounds, determine the key length (10, 12 & 14 rounds show the key length of 128, 192 & 256 bits). At last, shifted data into rows & columns (XOR operation performed in each column), longer data need more rounds.

## 4. TOOL, LANGUAGE&PACKAGE

In data security, multiples of algorithms design, implement, maintain & utilized but no one capable to handle numbers of threats in same time and restrict attacks on confidential information in network environment. There are many open-source programming language and tools available in market but in this research, we are choosing 'Python' as a high-level programming with 'Miniconda '&' Pycrypto' for cryptography

### 4.1. Python

High-level programming paradigm which has ability to build data structure, dynamic binding & typing, create attractive application development, and connect components together. Python is an object oriented, interpreted (interpret each line of codes) and dynamic semantic programming language. Syntax is readable, simple, and easy to use, reduce programming cost and maintainable. Program can be divided into different modules; each module can be used as an individual project. Python provides extensive standard library, which reduce the computational cost & increase efficiency. The edit-text-debug cycle is fast, debugging is easy, strong error detection & fault tolerance. Although. Python is user friendly programming language but also have lots of built-in functionalities i.e.(listing, dictionary, comprehension, creating corpus etc.) which makes python differ than others.[2]

### 4.2. Pycrypto

Pycrypto is the python cryptography toolkit, collection of hash function & encryption algorithms (DES, RSA, AES, and many more). The packagehas capability enhance new module easily. One of the essential module examples is AES, written secure administration tool. The package can be install by simply run 'python setup.py build' (build the package), after that run 'python setup.py install' on command prompt or it can also be installed by using 'Miniconda', run command 'conda install pycrypto'on 'Anaconda Prompt', it take less amount of time to completely install pycrypto in the system.[3]

## 5. RESULTS

In this section, the proposed solution can fix the entire problem of data confidentiality. The given solution encrypts crucial information from unauthorized person and decrypt only those which authorized by encrypted person, its mean that without symmetric keyit can't be access. In python pycrypto AES, there are some prime functions which help to provide confidentiality, integrity, controlling & availability. Encryption & Decryption of AES steps are as under:

Step #1: Fetch Pycrypto package and import AES algorithm using command 'from Crypto. Cipher import AES' **(Fig. 1).**

Step #2: Define encrypted function (user-define) with a parameter named 'hiddeninfo'. Convert plaintext into ciphertext, generate secret key which can only know by authorized person **(Fig. 2).**

Step #3: The encrypted key shared with those who are the responsible to decrypt sensitive information without alter it.

Step #4: Define decrypted function with a parameter named 'showinfo'. Convert ciphertext into plaintext and display information on the screen **(Fig. 3).**

In result, the complete image exhibit AES functionality and pivotal data security. Data integrity is critical component of data confidential; AES ensure the data confidentiality and create session between authorized access. Reduce spoofing concept and increase availability. At last, cryptography AES is the best for encryption &decryption purpose, execution perform with in a second, no delay, more file storage than other, accurate & efficient.

[1] https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

[2] https://www.python.org/doc/essays/blurb/

[3] https://pypi.org/project/pycrypto/

```
>>> encryption("my bank account number is 202123456 and passward is Abdullah")
encryption key: ¨ø|DgwêâïqEVÂü.
Encrypted string: oUJBu6uBUS6uu9mXCq4hWm9zjThaoKr7n8l2iubmh5uSBpnqAZDBCCi7ejTwOQA3xaPiLZkxnceAe2N+B822sA==
>>>
```

***Fig. 1- Encryption of AES***

```
>>> decryption('oUJBu6uBUS6uu9mXCq4hWm9zjThaoKr7n8l2iubmh5uSBpnqAZDBCCi7ejTwOQA3xaPiLZkxnceAe2N+B822sA==')
Decrypted string: my bank account number is 202123456 and passward is Abdullah
>>>
```

***Fig.3- Decryption of AES***

## 6. CONCLUSION

Data Confidentiality is rising as a challenging task nowadays, researchers try to find different ways to overcome the problem but unfortunately, it's still the condemnatory issue. Secure communication path between sender & receiver is the prime factor of data security. Cryptography perform a vital role to restrict unauthorized access in network domain. In cryptography, evolving two major parts, such as encryption used for encoding text into special characters known as cipher text, and decryption used to retrieve information known as plaintext. The problem arises when choosing algorithm in the bulk of encrypted algorithm, mainly focus on strong security. Result shows that the successfully design, implement, management, controlling & utilization of AES in python is the protected solution for confidential communication At the end, AES gives more security with accuracy and provide a communication path where information can travel one to another authorized access without disturbing data integrity, confidentiality, availability & access controlling.

## REFERENCES:

Arunkumar, R. Josephius, and R. Anbuselvi. (2017). "Enhancement of Cloud Computing Security in Health Care Sector.

Aljawarneh, S and M B. Yassein. (2017) "A resource-efficient encryption algorithm for multimedia big data." Tools and Applications 76. 21, 22703-22724.

Çavuşoğlu, U., (2018) "A novel hybrid encryption algorithm based on chaos and S-AES algorithm. " Nonlinear Dynamics 92.4: 1745-1759.

Dakhare, B., (2018). "Performance Analysis of Data Encryption Algorithms using AES BLOWFISH and SNAP. "International J, of Engineering Science 16466.

Li, Y. (2017): "Intelligent cryptography approach for secure distributed big data storage in cloud computing." Information Sciences 387 103-115.

Patil, P (2016): "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science 78 617-624.

Pandey, R. M., and V. K. Verma. (2015). "Data Security using Various Cryptography Techniques: A recent Survey.

Sivakumar, R., B. Balakumar, and V. Arivu (2018). Pandeeswaran. "A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security."