Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 3– No.4, November 2015 – www.caeaccess.org

Implementation and Performance Evaluation of the AES Algorithm for Data Transmission using Various Programming Languages

Binal Shah
Information Technology
Thakur College of Engg. & Tech.

Zahir Aalam
Information Technology
Thakur College of Engg. & Tech.

ABSTRACT
Due to the speedy development of digital communication and electronic data exchange, data security and performance have become a crucial issue in the industry, business and government. Cryptography provides essential techniques for ensuring data and protecting information. Advanced Encryption Algorithm (AES) is one of the encryption techniques which protects data and it is used most frequently because of its high efficiency and simplicity. Programming Languages (PL) can be utilized to produce plans to control the behavior of a machine or to express algorithms. To improve the Performance of digital communication, PL is also one of the important elements because the ability of the compiler to perform optimizations is directly associated to the language specification. This paper gives the outline of comparison between 3 different Programming Languages based on AES algorithm. The comparison is for which languages are more efficient in run-time execution speed. Programming Languages used in the comparison are MATLAB, JAVA and C#. Evaluation is done using Encryption Time, Decryption Time and Throughput.

General Terms
Cryptography Algorithm, Programming Languages

Keywords
AES, C#, JAVA, MATLAB

1. INTRODUCTION
The Internet is everywhere now! Always online. All over IP. These buzzwords point out that at one time more extensive changes are coming out in the area of telecommunications networks. The recent growth in competition, new requirements of the securities industry and technological developments have fundamentally altered the traditional positions of the telecoms industry. The present industry is qualified by the rapid development of broadband connections, the convergence processes of several network technologies and the emersion of a uniform IP standard for individual and mass communications. The thought behind Next Generation Networks (NGN) is picking up importance and presents new challenges.

According to ETSI, NGN is a concept for defining and installing of the webs, which allows a formal distribution of functionalities into separate layers and planes which makes use of open interfaces and thus making it possible for the service providers and operators to create a program which can be gradually built up thanks to the creation, implementation and efficient management of innovative services [1], [2]. ITU-T defines NGN [3] as a network based on packet transfer, enabling to provide services, including telecommunication services, and is capable of using several broadband transmission technologies allowing guaranteeing QoS. NGN provides unlimited user access to different service providers. It supports general mobility providing the users with consistency and accessibility of services.

To consider Next Generation Networks essentially as an innovation would be an erroneous over simplification. In fact, the network operator is pushed to get new base architectures and administration suppliers' new plans of action. NGN implies that enterprises must think about how to present the novel innovation and how they relocate from ordinary plans of action to NGN business models. The Next Generation Networks administration reach will be altogether more extensive than that of ordinary information transfer systems. New or extra included quality potential outcomes develop. Online content will be made accessible all the more effective, rapidly and promoted all the more broadly. Since NGN has open and standardized interfaces, fast execution and incorporation of new functions and services is possible. The user can answer this straight without having to experience the network architecture.

2. CRYPTOGRAPHY ALGORITHM
Cryptography could be a science that applies complicated arithmetic and logic to design robust secret writing ways. Achieving robust secret writing, the hiding of data's meaning. Cryptography could be a cornerstone of the trendy electronic security technologies used these days to protect valuable information resources on intranets, extranets, and also the web. Cryptography is a system for saving and transmitting information in a specific frame so that those for whom it is proposed can read and process it.

AES (Advanced Encryption Standard) is a symmetric block cipher utilized by the U.S. government to make sure of classified data and is used everywhere in software and hardware to turn key information into a secret code (encryption). AES contains three block ciphers, 128 bits AES, 192 bits AES and 256 bits AES. Information would encrypt and decrypt by block of 128 bits using keys of 128,192 and 256 bits, respectively. For encryption and decryption, similar key is used by Symmetric or secret-key ciphers. So the same secret key should be known and used by both, the sender and the receiver. To secure classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths, every single key length is considered to be sufficient. There are 10 rounds for 128-bit

keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Around is comprised of a few preparing steps that incorporate substitution, shift rows and mixing of the input plain text and convert it into cipher text. The four steps that compose the standard round are:

• Substitute bytes: nonlinear procedure that uses the S-box to perform byte by byte of the data block.

• Shift rows: a simple transformation that uses permutation to shift the bytes within the data block in cyclic fashion.

• Mix columns: a simple transformation that uses arithmetic over 8 GF (2^8) to group 4-bytes together forming 4-term polynomial, then multiplies the polynomials with a fixed polynomial 4*4 matrix.

• Add round key: bitwise XOR of the current block with a portion of the expanded key.

The encryption and the decryption structure of the AES algorithm with four steps are as shown in Fig. 1.

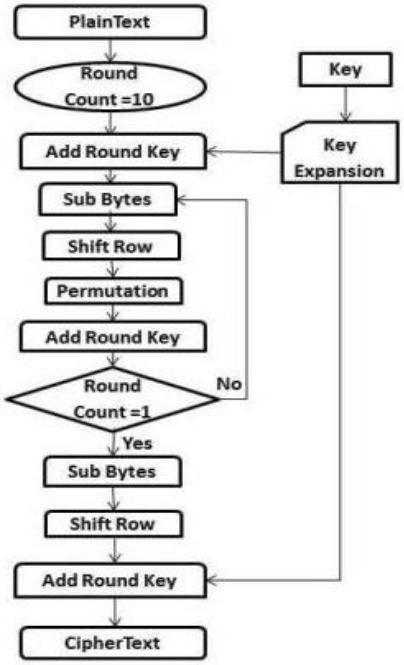

Fig. 1: Flow chart of AES Algorithm

3. PROGRAMMIMG LANGUAGES

Programming languages are those languages, which refers to a means of expressing computations in a form comprehensible to both the people and machines. Various sorts of phrases such as expressions, commands, declarations, and so forth may be combined to form programs by means that is specified by the syntax of a language . Programming languages are used by software engineers to compose instructions that a computer can understand to do what the developer needs. Machine language is the most fundamental (called low-level) coding that uses binary ('1' and '0') code run by a computer quickly without utilizing any interpreter or mediator program. But however, it is tedious and complex. The various high-level programming languages such as C#, C, Java are easy to use, but require use of another program (called a compiler or an interpreter) to convert the high-level code into the machine code. New programming languages are continuously developing and also large no. of languages are already existing. In the present study, three languages are studied, namely C#, Java and Matlab.

3.1 C#

C# is a modern object-oriented, general-purpose programming language, created and developed by Microsoft together with the .NET platform. There is a highly diverse software developed with C# and on the .NET platform: office applications, web applications, websites, desktop applications, mobile applications, games and many others. C# is a high-level language that is similar to Java and C++ and, to some extent, languages like Delphi, VB.NET and C. All C# programs are object oriented. They consist of a set of definitions in classes that contain methods and the methods contain the program logic – the instructions which the computer executes [6]. It presents some unique and capable components, for example, delegates (which can be viewed as a type-safe function pointers) and lambda expressions which present components of functional programming languages, as well as a less complex single class inheritance model (than C++) and, for those of you with involvement in "C-like" languages, an exceptionally well known syntax that may help beginners get to be capable speedier than its predecessors. C++ supports exception handling, multiple types of polymorphism, and separation of interfaces from implementations. Certain features which are combined with its intense advancement tools, multi-platform support, and generics, make C# a good choice for many types of software development project like Internet applications, fast application development projects, projects with strict reliability requirements projects and implemented by individuals or large or small teams. Its strong writing helps to prevent many programming errors that are common in weakly typed languages.

3.2 Java

Java is a high-level programming language initially created by Sun Microsystems and released in 1995. Java runs on a various platforms like Mac OS, the various versions of UNIX, and Windows. The primary goal of the Java language Java was originally designed by its developers to be: 1. Simple, object oriented, and familiar 2. Robust and secure" 3. Architecture neutral and portable 4. Able to execute with high performance 5. Interpreted, threaded, and dynamic [7]. The plan for "write once, run anywhere" (WORA), implying that compiled Java code can run on any platforms that support Java without any recompilation. Java applications are compiled to byte code that can run on any Java virtual machine (JVM) regardless of computer architecture. As of 2015, for developing the client-server web applications, Java is one of the most popular programming language which is used.

3.3 Matlab

MATLAB is a programming language developed by Math Works. MATLAB is a high-level language and interactive environment for numerical computation, visualization, and programming. Using MATLAB, one can analyze data, develop algorithms, and create models and applications. The language, tools, and built in math functions enable you to explore multiple approaches. Applicability range of MATLAB is which includes signal processing and communications, image and video processing, control systems, test and measurement, computational finance, and computational biology. The language of technical computing,

i.e. MATLAB is used by more than a million engineers and scientists in industry and academia [8].

4. EVALUTION PARAMETERS

Evaluation is the organized interpretation and giving of intending to predict or real impacts of recommendations or results. It looks at original objectives, and at what is either anticipated or what was accomplished and how it was accomplished. So evaluation can be formative that is occurring amid the advancement of an idea or proposal, project or association, with the goal of improving the quality or effectiveness of the proposal, project, or organization.

In this paper, Evaluation is done using following parameters.

Encryption Time: Encryption is the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties. It may also be performed with a set of keys or passwords. The time taken to encrypt any file is called Encryption Time. Here, Encryption Time is measured in milliseconds (ms).

Decryption Time: Decryption is the process of transforming data that have been rendered unreadable through encryption back to its unencrypted form. During decryption, the system extracts and converts the cipher data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. It may also be performed with a set of keys or passwords. The time taken to decrypt any file is called Decryption Time. Here, Encryption Time is measured in milliseconds (ms).

Throughput: Throughput is a key measure of the quality of a network. It is defined as the number of information bits received without error per second and this quantity is suited as high as possible [9]. Here, Throughput is measured in Mbps (Megabits per second).

5. RESULTS AND DISCUSSION

The result carried out is based on encryption and decryption time and throughput. Computer Configurations used are Microsoft Windows 8.1, Intel (R) Core (TM) i5-4210U CPU @ 1.70 GHz, 2.40GHz, 8 GB RAM.

Programming Language configuration:

C#:

Software: Microsoft visual studio 2010,

Framework: .NET.

JAVA:

Software: NetBeans IDE 7.2

Jdk: 1.7.0

MATLAB:

Software: MATLAB R2013a

- **ENCRYPTION AND DECRYPTION TIME**

Encryption time and Decryption time of TEXT file using AES (128-bit) Algorithm:

Size of Text file: 18.6 KB

Table 1 gives the information about the encryption time and decryption time of Text file taken by AES algorithm using different Programming languages like Matlab, Java and C# for the data transmission.

Table 1. Encryption Time and Decryption Time of TEXT file

Programming Language	Throughput	
	Encryption time (Milliseconds)	Decryption time (Milliseconds)
Matlab	143	120
Java	99	77
C#	66	43

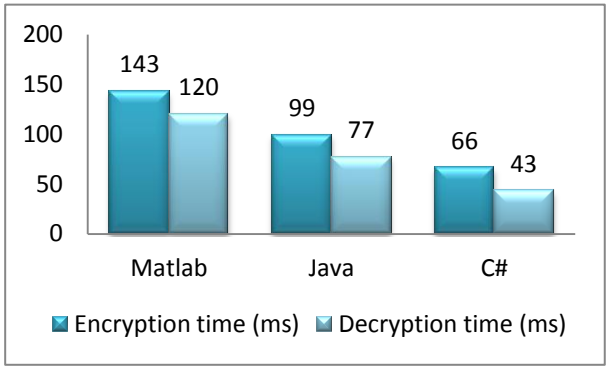

Fig. 2: Graphical representation of Encryption Time and Decryption Time of TEXT file

Fig. 2 shows that the C# language takes less time than the Matlab and Java for encryption and decryption process of the Text file.

Encryption time and Decryption time of IMAGE file using AES (128-bit) Algorithm:

Size of Image file: 39.7 KB

Table 2 gives the information about the encryption time and decryption time of Image file taken by AES algorithm using different Programming languages like Matlab, Java and C# for the data transmission.

Table 2. Encryption Time and Decryption Time of IMAGE file

Programming Language	Encryption time (Milliseconds)	Decryption time (Milliseconds)
Matlab	1145	915
Java	308	215
C#	95	80

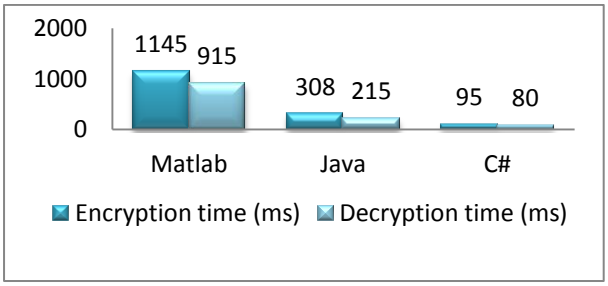

Fig. 3: Graphical representation of Encryption Time and Decryption Time of IMAGE file

Fig. 3 shows that the C# language takes less time than the Matlab and Java for encryption and decryption process of the Image file.

Encryption time and Decryption time of AUDIO file using AES (128-bit) Algorithm:

Size of Audio file: 2.74 MB

Table 3 gives the information about the encryption time and decryption time of Audio file taken by AES algorithm using different Programming languages like Matlab, Java and C# for the data transmission.

Table 3. Encryption Time and Decryption Time of AUDIO file

Programming Language	Encryption time (Milliseconds)	Decryption time (Milliseconds)
Matlab	15510	14185
Java	12119	11544
C#	3903	7896

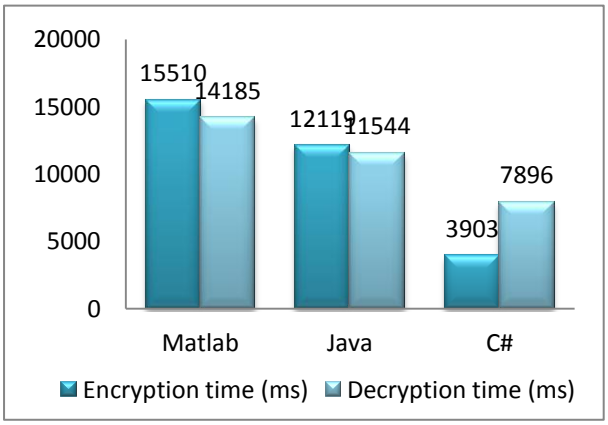

Fig. 4: Graphical representation of Encryption Time and Decryption Time of AUDIO file

Fig. 4 shows that the C# language takes less time than the Matlab and Java for encryption and decryption process of the Audio file.

Encryption time and Decryption time of VIDEO file using AES (128-bit) Algorithm:

Size of Video file: 3.73 MB

Table 4 gives the information about the encryption time and decryption time of Video file taken by AES algorithm using different Programming languages like Matlab, Java and C# for the data transmission.

Table 4. Encryption Time and Decryption Time of VIDEO file

Programming Language	Encryption time (Milliseconds)	Decryption time (Milliseconds)
Matlab	35412	31854
Java	16214	15776
C#	5882	11321

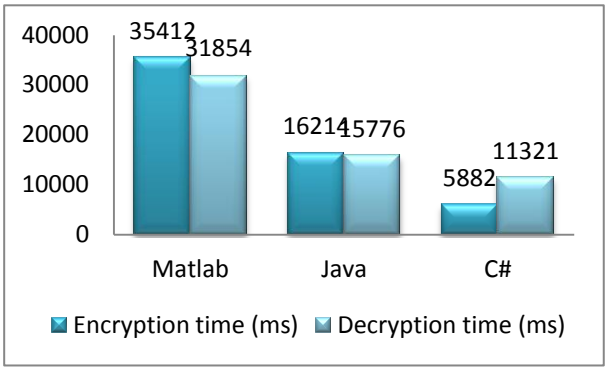

Fig. 5: Graphical representation of Encryption Time and Decryption Time of VIDEO file

Fig. 5 shows that the C# language takes less time than the Matlab and Java for encryption and decryption process of the Video file.

- **THROUGHPUT**

Throughput of TEXT File

Throughput = bits/Second

Table 5 gives the information about the Throughput of encryption and decryption time of Text file using different Programming languages like Matlab, Java and C#.

Table 5. Throughput of TEXT file

Programming Language	Throughput	
	Encryption (Mbps)	Decryption (Mbps)
Matlab	0.133	0.166
Java	0.494	0.708
c#	1.603	1.904

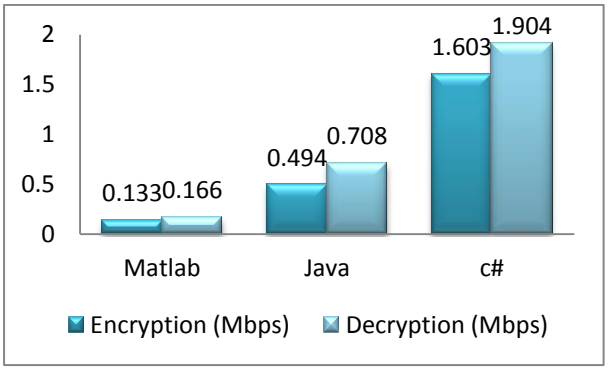

Fig. 6: Graphical representation of Throughput of TEXT file

As shown in Fig. 6, C# gives better throughput for the Text file than the Matlab and Java.

Throughput of IMAGE File

Throughput = bits/Second

Table 6 gives the information about the Throughput of encryption and decryption time of Image file using different Programming languages like Matlab, Java and C#.

Table 6. Throughput of IMAGE file

Programming Language	Throughput	
	Encryption (Mbps)	Decryption (Mbps)
Matlab	0.284	0.355
Java	1.055	1.512
c#	3.423	4.065

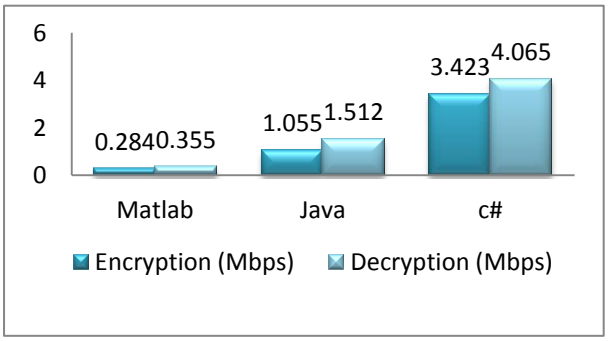

Fig. 7: Graphical representation of Throughput of IMAGE file

As shown in Fig. 7, C# gives better throughput for the Image file than the Matlab and Java.

Throughput of AUDIO File

Throughput = bits/Second

Table 7 gives the information about the Throughput of encryption and decryption time of Audio file using different Programming languages like Matlab, Java and C#.

Table 7. Throughput of AUDIO file

Programming Language	Throughput	
	Encryption (Mbps)	Decryption (Mbps)
Matlab	1.481	1.620
Java	1.896	1.910
c#	5.889	2.910

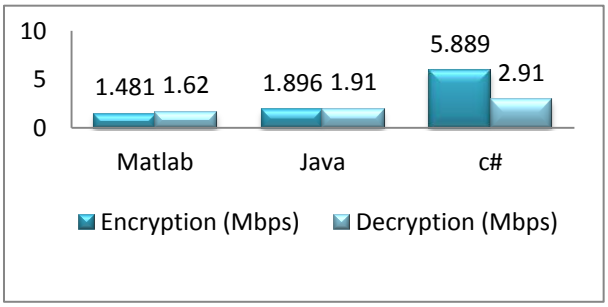

Fig. 8: Graphical representation of Throughput of AUDIO file

As shown in Fig. 8, C# gives better throughput for the Audio file than the Matlab and Java.

Throughput of VEDIO File

Throughput = bits/Second

Table 8 gives the information about the Throughput of encryption and decryption time of Text file using different Programming languages like Matlab, Java and C#.

Table 8. Encryption Time and Decryption Time of VIDEO file

Programming Language	Throughput	
	Encryption (Mbps)	Decryption (Mbps)
Matlab	0.883	0.982
Java	1.929	1.983
c#	5.321	2.763

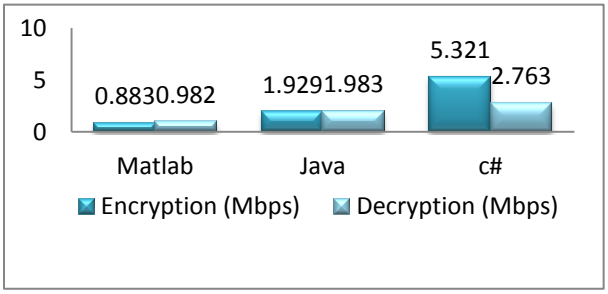

Fig. 9: Graphical representation of Throughput of VIDEO file

As shown in Fig. 9, C# gives better throughput for the Video file than the Matlab and Java.

6. CONCLUSION

Programming Languages are the main factors to improve the execution of some applications and hence a solution has to be proposed on the different languages like MATLAB, JAVA and C#. Present paper provides a solution based on AES algorithm. Text and Image files are encrypted and decrypted using AES algorithm and then how much time is required by AES to encrypt and decrypt a file is counted on. Encryption and decryption time taken by C# language is less as compared to JAVA and MATLAB whereas JAVA took more time than C# and less as compared to MATLAB. Also, the time taken by MATLAB is more as compared to the other two languages, i.e. JAVA and C#. It could also be observed from the above results that the C# language gives better throughput than the JAVA and MALAB. Also, C# gives better performance for providing with evaluation parameters. Hence, it could be concluded that the C# language is more efficient at run time execution speed as compared to the other two languages used namely, JAVA and MATLAB.

7. ACKNOWLEDGMENT

I receive immense pleasure in presenting the paper on "Implementation and Performance evaluation of the AES algorithm for data transmission using various Programming Languages". I take this opportunity to convey my sincere thanks to Mr. Vikas Kaul. I' am also grateful for the invaluable support given by my family and staff of the Information Technology department.

8. REFERENCES

[1] Podhradsky, Pavol Mikoczy, Eugen Labaj, Ondrej Londak, Juraj Truchly, Peter, " NGN Architectures and NGN Protocols, LdV IntEleCT, Educational publication, 210 pages, ISBN:978-80-01-04949-5, September 2011.

[2] Mikoczy, Eugen Podhradsky, Pavol Matejka, Juraj Labaj, Ondrej Tomek, R. Kadlic, Radoslav Schumann, Sebastian Massner, Schuman Dungel, M. Kotuliak, Ivan Mikula, J, "NGN Protocols," LdV Projekt Train2Cert, 2008.

[3] ITU-T, SG13, NGN 2004 Project description, Vol 3, 2004

[4] Vishal Pachori, Gunjan Ansari, Neha Chaudhary, "Improved Performance of Advance Encryption Standard using Parallel Computing," International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 1**,** 2012.

[5] Robert Harper. Practical Foundations for Programming Language. Carnegie Mellon University

[6] Svetlin Nakov, Vaselin Kolev & Co.Fundamentals of computer programming with C# 2011.

[7] Iván Devosa, András Erik Csallner. Introduction to Java Programming Language. Course book, Applications of Informatics Department, University of Szeged, JGYF Press, Szeged, 2010.

[8] MATLAB® Primer, 1984–2015 by The MathWorks, Inc.

[9] Youssef Fakri, Benayad Nsiri, Driss, ABOUTAJDINE, Josep VIDAL. Adaptive Throughput Optimization in Downlink Wireless OFDM. I. J. Communications, Network and System Sciences. 2008.