March - April 2020
ISSN: 0193-4120 Page No. 11480 - 11487

Intrusion Detection USINGC-AES (Complimented Advanced Encryption Standard) Algorithm

[1]Prerit Kaliraman, [2]Rohit, [3]Renuka Devi P

[3]Assistant Professor, [1,2,3]Department of Computer Science and Technology,
SRM Institute of Science and Technology
[1]prerit1026@gmail.com, [2]rsuhag999@gmail.com, [3]renukadevi.p@ktr.srmuniv.ac.in

Article Info
Volume 83
Page Number: 11480 - 11487
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 16 April 2020*

Abstract

An intrusion detection system monitors a network and detects any conduct out of the example or any sort of unapproved access in the system. It is a system danger counteraction innovation observing system traffic stream and recognizes weak areas in a framework. The work of these systems is to observe the network traffic and report any deviation from regular traffic flow. The anomalies or deviation are based on the pattern or a model used for identification or classification of an intrusion. The objective of the project is to create an intrusion detection system that monitors a network and detects any behaviour out of pattern or any unauthorized access in the network. People do spend a lot of time on the internet indulging themselves in some kind of activities usually with less secured networks or networks that can be easily penetrated. The purpose for this project has arisen due to the number of attacks on host, network systems such as the WannaCry Ransom ware and lack of their adaptability to new types of system attacks. It is a network threat prevention technology monitoring network traffic flow and detects vulnerable points in a system. An ID is classified on the basis of the location it is put in. The work of these systems is to observe the network traffic and report any deviation from regular traffic flow. The anomalies or deviation are based on the pattern or a model used for identification or classification of an intrusion.

Keywords: *IDS, NIDS, HIDS, IOT, OSI, D-o-S, U2R, ABC, ATIDS, JSP*

1. Introduction

With the growing importance and reliability on computers as well as the internet and unprotected networks such as Bluetooth or Wi-Fi the need for cyber security is much more prominent and in demand. With the interconnected nature of today's society and their reliability on the internet and devices that are a part of IOT cyber-attack are the biggest threat today. Every modern company today relies on the internet, all transactions, communications, personal and private information although not available to the public are still hosted on the internet. In today's world information is power and ranging from a common person to a president everyone uses the internet and is vulnerable to cyber-attacks. Anyone having access to another person's secrets can easily exploit them. These people are generally referred to as hackers which make it ever so vital to enhance cyber security. Any application or device that is capable of monitoring and protecting a network from a likely intruder can be termed as an Intrusion detection system. IDS are mostly used in network related activities to reduce the risk of intrusion by any unauthorized party. The function of the intrusion detection system is to monitor a network and detect any behaviour out of pattern or any unauthorized access in the network. While firewall do a good job of monitoring traffic coming from the internet but they cannot detect if the network provider itself has been changed but rather just the traffic flow.

March - April 2020
ISSN: 0193-4120 Page No. 11480 - 11487

2. State of the art (Literature Survey)

YEAR	AUTHOR	TITLES	PROPOSED COUNTER MEASURES	FINDINGS/DRAWBACKS
2018	Subbalakshmi T, Suryansh Bhardwaj, Prakhar Ranjan and Kenneth Antony John	Enhanced SPK Encryption Algorithm for File Encryption using Java	Using SPK algorithm for encryption of files within a secured network.	Not fast as compared to AES or other encryption algorithms and Security is also low.
2018	1 Meetender, 2 Nirbhaya Kashyap, 3 Archit Aggarwal, 4 Tanupriya Choudhury	Security techniques using Enhancement of AES Encryption	Using S-box to enhance the strength of cryptographic data.	Full data is not encrypted, only parts of sensitive data is encrypted.
2017	FlevinaJonese D'Souza Dakshata Panchal	AES)Security Enhancement using Hybrid Approach	Creating confusion and diffusion in cypher text to avoid attackers to know S-box size and values.	Complex algorithm. As it uses shift and mix transformation of rows on data.
2014	Debiao He Ding Wang	Robust Biometrics-Based Authentication Scheme	New Authentication Scheme for Multi-server	Unable to find a way to protect Biometrics to become imitated and cannot protect Smart cards ID to be stolen and used to data-bifurcation
2014	H. Hakan TugrulYanik	SIP Authentication and Key Agreement Server	Using Key Authentication to avoid attacks, Different cryptographic techniques such as Hash and Symmetric Encryption based Schemes, ID based Schemes	MIME, HTTP digest authentication TLS and Secure Real Time Transport Datagram Transport Layer All these things have issues as they are susceptible to attacks and cannot be protected from that.
2014	Hyun Sung Kim	ID based Password Authentication Scheme using Smart Cards and fingerprints	Using ID based Authentication scheme that does not refer dictionary of passwords or verification table, i.e.- [a] ID [b] Password [c] Fingerprint	Time Stamp based authentication messages are susceptible to replay attacks.
2008	Yan-Yan Wang Jia-Yong Lin Jing Dan	A More efficient and Secure Id-based Authentication	ID-based authentication scheme to enhance the security	It could not resist impersonating a server attack.

March - April 2020
ISSN: 0193-4120 Page No. 11480 - 11487

2005	Kyu Young Chai Jung Yeon Hwang Dong Hoon Lee In SeogSeo	ID-based Authenticated Key Agreement	authentication by using Bilinear Maps	difficult to implement ID based authentic Key Agreement on Low Power Mobile Device
2004	Mainak Lal Das Ashutosh Saxena	Dynamic ID based Remote User Authentication Scheme	Dynamic ID-based scheme that can resist the reply attacks, forger attacks, guessing attacks and insider attacks	Unable to maintain any verifier table verifying validity of user details at once Eliminates the remote system's overheads.

3. Implementation

FRONTEND: Introduction of Java: Java was developed by Sun Microsystems UN 1991. It is a compiled and interpreted language; deriving features from C and C++ making it a pure object-oriented programming language. It has various features like platform independence and is capable of graphics and networking. Two types of programs can be created using Java – namely applications and applets. A program running under a working framework on a PC is an application like an application made utilizing C or C++. Some of the highlights of Java are

Object - Orientation, Robustness, High Performance, Security, Portability and so on

J2EE: - It depends on programming running on java application server. It can be defined as the programming platform for development and running of multi-tier architecture java applications.

TOMCAT: -Primarily used in web-applications, its main function is to act as a cross platform application server Servlet and JSP specifications are implemented by it.

SERVLET: - Java language objects utilized for dynamic handling of solicitations and build reactions are known as Servlets. Javax. servlet and javax. servlet. http bundles contain the Servlet API. Java server Pages (JSP) compiler is utilized to consequently create servlets.

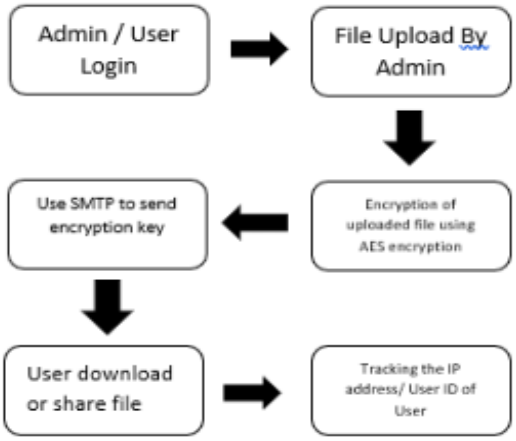
Net Beans: -It is the most complete Java comprehensive Java version coordinated improvement condition for the open Source Net beans stage. Giving an improvement domain to WEB-XML, databases and application server connectors for streamline advancement, testing and transportability.

Back END: Structure Query Language (SQL): - SQL is a question language for relational database for recovering a record from the social database utilizing a non-method approach. Originally proposed by IBM and after getting standardization by ANSI it was adopted by different corporations with modifications according to the corporation needs. It can be divided into three categories:

DML – Data Manipulation Language: - Often a sublanguage of database languages, DML is used for manipulation of the relational database involving functions such as adding, deleting and modifying the contents of the database. Its primary use is to retrieve records from the relational database.

DCL - Data Control language: - Often a sublanguage of database languages, DCL is similar to a computer language in the sense that it is used to grant or revoke privileges from the user, these privileges may include select, insert etc.

DDL – Data Definition language: - Often a sublanguage of database languages, DDL is used to define data structures and schemas pertaining to databases. Some of the command may include permissions to create and change tables such as create, alter, drop and truncate.



Design and Implementation

Overview of Concept

JAVA

Initially known as OAK, java was developed by Sun Microsystems un 1991. It is a compiled and interpreted language, deriving features from C and C++ making it a pure object-oriented programming language. It has various features like platform independency and is capable of graphics and networking.

Two types of programs can be created using Java – namely applications and applets. A program running under an operating system on a computer is an application similar to an application created using C or C++. Java provides the Java Virtual Machine (JVM).

Some of the features of Java are Object -Orientation, Robustness, High Performance, Security, Portability etc.

March - April 2020
ISSN: 0193-4120 Page No. 11480 - 11487

JAVA Database Connectivity

To execute SQL statements, Java uses an application interface known as Java database connectivity (often abbreviated as JDBC) consisting of classes and interfaces written in Java language.

It provides ease of use to send any SQL query to a relational database. In other words, using JDBC we can write a single program to access all the databases rather than write an individual program for each database and design the functionality of the program such as it is able to send the SQL queries to the appropriate database. Java and JDBC combination allow a program to be written once and due to the portable nature of java, it can be run from anywhere.

Java features such as its robustness, security, ease of use, and automatic downloading on any network, provides a good base for database applications.

JDBC can be considered an extension to Java as it extends a lot of the functionality of Java.Everybody can access an application written by a programmer when put on the server, and they have to write it only once and then upload it.

JDBC is easy to use and is considered a low-level interface because of its functionality to directly invoker SQL commands, it works well in this capacity and is easy to use as compared to other database application interfaces. However, its purpose of design was to be a base to build high level interfaces. A high-level interface uses a more convenient application interface that performs all the translations to low level behind the scenes. It is highly user friendly and usually contains some sort of a UI.

A harder to learn database tool is ODBC. One of the reasons for that is the ODBC mixes both simple and advanced features causing there to be multiple and complex options regarding even the simplest of queries. In contrast to this, JDBC was designed to keep things simple while leaving room for advanced features according to the project or organization requirements.

To enable a pure java solution a Java Application interface like JDBC is required, while in the case of ODBC all its drivers must be installed manually on each client system. However, if the driver software for the JDBC is completely written in Java, owing to the features of Java it becomes installable, portable and secure as well as platform independent.

Database Management System (DBMS)

A Database is an integrated collection of client/user related information stored with least repetition, serving numerous clients/applications rapidly and proficiently. A database system is essentially a record keeping system, i.e. it is an automated system whose general reason for existing is to keep up data and make that data accessible on request.

DBMS is mainly divided into-

1. Database: It is an integrated collection of client/user related information stored and used by the application system.
2. Hardware: The main memory and hardware such as processor, ram, ports and servers used to maintain and execute the databases.
3. Software: It is the medium through which the user accesses the database from the physical components and passes all the requests from the user to the database.
4. User: Mainly there are three types of users, i.e. Database administrator, End user nd Application Programmers.

Relational Database Management Systems

Database Management System initially started with hierarchical models slowly evolving to the network models and finally to relational models and most accepted database model is the relational database. This model manages the database using only its relational capabilities. It consists of three different aspects namely – Structures, Operation and Integrity rules. These can be defined as follows:

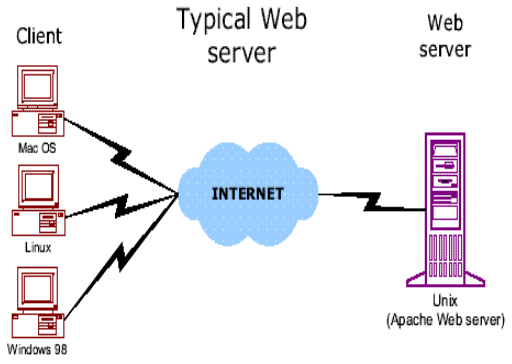
Structures: The data of the structure of a database is stored in well-defined objects known as Structures. Operations can be performed on structures to manipulate the data stored in them.

Operations: Operations are commands or actions that allow a client/ user to manipulate the data stored in database. They can also be used to manipulate the structure of a database.

Integrity rules: Integrity rules are predefined rules that database operations must follow.

Java Server Page (JSP)

It is one of the server-side Java technologies, Java Server Pages (JSP) allows software developers in creation of dynamic web pages, extensions such as HTML, XML or other document types. JSP compiler is used to compile JSP into servlet.



JSP is used by a client to perform a web service that depends on the J2EE application and is similar to a java servlet in design and functionality. The difference however is in the programming of the servlet and JSP. While a servlet comprises mainly of programming

March - April 2020
ISSN: 0193-4120 Page No. 11480 - 11487

language Java, the JSP is written in the HTML, XML or a web page extension.

When a JSP is requested, three methods namely - jspInt, jspDestroy and service - methods are automatically called. Termination of JSP is normal.

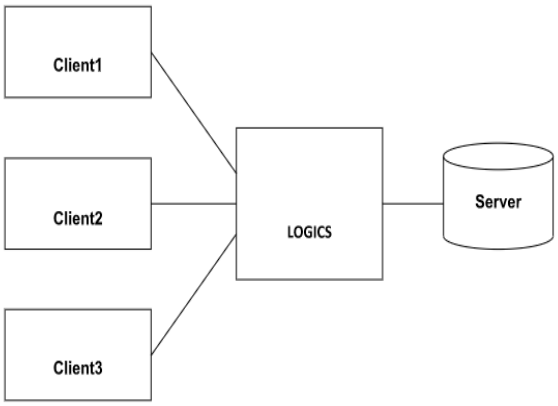
The jspDestroy method is called when jsp terminated while when connection to HTTP needs to be retrieved the service () method called.

A virtual machine running on a web server is used to execute jsp programs. Therefore, a virtual machine such as Apache or TOMCAT is needed to execute JSP.

Java Server Pages (JSP) allows software developers in creation of dynamic web pages, by providing development models and help in implementation of server-side technologies such as databases, caching etc. Other technologies such as ASP, ColdFusion and PHP provide support for similar models none offer JSP advantages.

JSP Architecture

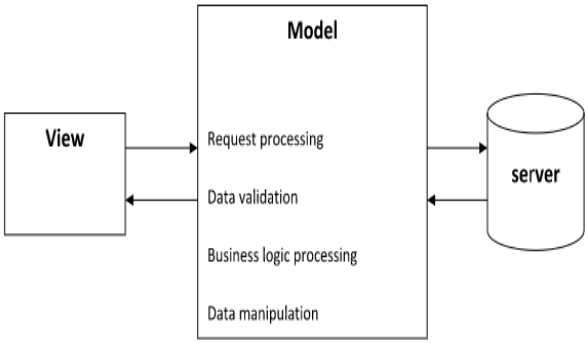
In order to make content generation dynamic, a new concept known as "Logic separation" from the client is introduced.



Logic like programs is written and uploaded to the server and can then be accessed by all the users according to their requirements. Two architectures are known in order to implement this: -

Model-1:

Model-1, combines business and presentation logic and each logic requires the copy of the other and in order for the server and model to work towards this a lot of time and resource is consumed.



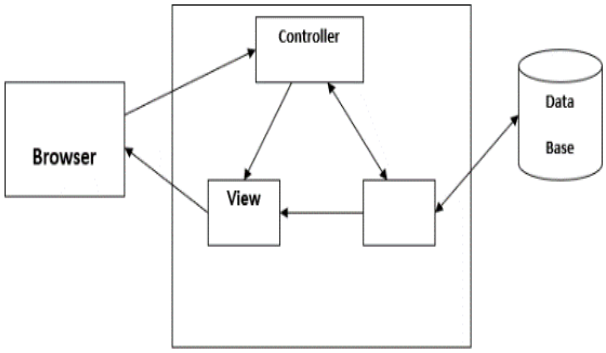
Model-2:

Model-2 also known as Struts. Both the business and presentation logics are separated in this model and it consists of three parts namely – Model, View and Controller.

Model: The model represents a database with an application state containing business logics.

View: Java Server Pages act as a view and these do not contain any data manipulation objects or commands.

Controller: Performs all the client/user functionality including information providing to JSP pages and control passing to views.



JAVA Servlets

It is a server-side program and it contain the business logic for processing a request called by the UI or another J2EE part. A request containing implicit-explicit information is sent from a client to server-side program which is then processed and another set of implicit-explicit information is reverted back.

Information generated by the UI or entered by the user themselves is known as explicit data. The server information such as HTTP information that a client generates not a user is known as Implicit data.

Advantages of java servlets

1. Even if there are multiple simultaneous requests the JVM only loads a single copy of Java Servlets.
2. Due to the persistence feature of a Java servlet, it remains active after request.

List of Modules:

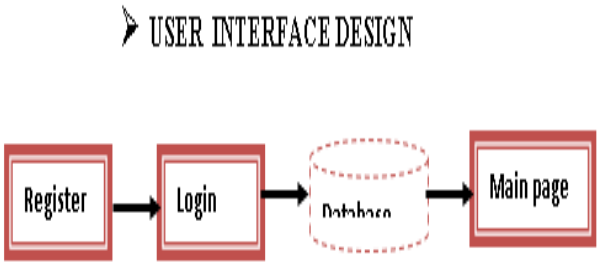
1 Admin Login
2 File Upload
3 Encryption

March - April 2020
ISSN: 0193-4120 Page No. 11480 - 11487

4 SMTP for sending encryption Key
5 User download or share file
6 File Tracking

ADMIN login: -

There is a login page for admin as well as registered users to login to the network portal hosted on a localhost using a WAMP server. The login page can be used to register a new user and the admin has privileges to put certain access specifiers on user status for need to know documents.



File Upload:-

Files / documents are uploaded by the admin and stored on the local server or the localhost. The same can be done when the project is implemented on the cloud or on the company server.

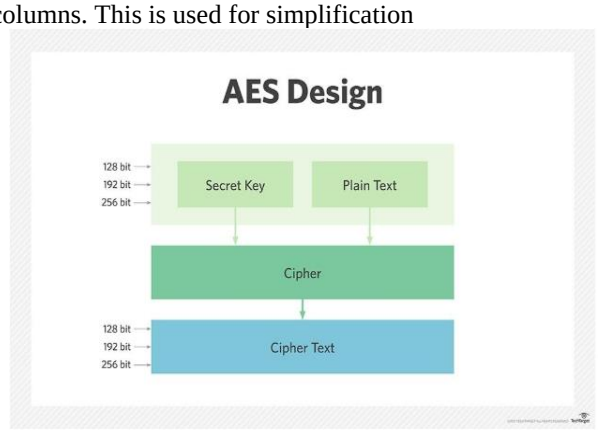
SMTP for sending Encryption Key: -

Gmail SMTP is used to send and receive the encryption key to authorized user created in above module

Encryption-

The admin uploads documents to share over the network and each file is encrypted using AES encryption with SPK encryption.

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. The AES Algorithm consists of a number of operations linked together in series, such as permutations and substitutions. The Proceedings of the algorithm is performed on its bytes rather than individual bits. So, these 128 bits of a plain text block are treated as 16 bytes. These 16 bytes are used as a matrix by placing them in 4 rows and 4 columns. This is used for simplification



User Download or Share File-

Authorised users can download the files uploaded by the admin and can also share the files with other users.

Tracking User-

Tracking user who have downloaded or access to the files IP addresses of the user who have downloaded the files have been recorded.

Proposed Work

The Proposed System works on a combined encryption algorithm based on AES and SPK (Suryansh Bhardwaj, Prakhar Ranjan and Kenneth Antony John) encryption algorithms. The fundamental idea of the project is to implement both SPK and AES encryption together.

SPK algorithm idea is that we first make a copy of the original file and then delete the original file. Now on the copied file step done is to convert all the data present in the file into bytes. Now since it is represented in the form of bytes for the encryption process, we take the compliment of it. Then the file extension is also changed according to the one who writes the code. For decryption we just do the opposite which is taking the complement again and then reverting the file extension.

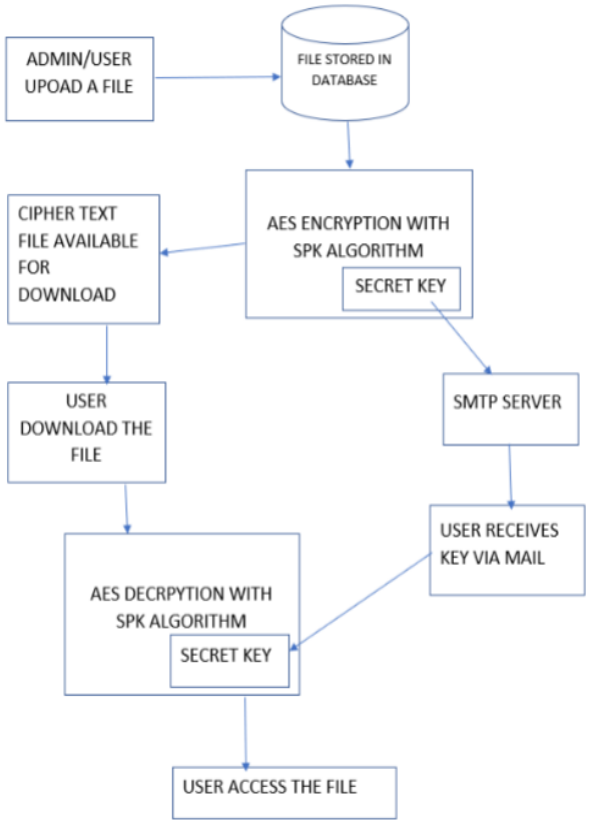
The AES Algorithm consists of a number of operations linked together in series, such as permutations and substitutions. The Proceedings of the algorithm is performed on its bytes rather than individual bits. So, these 128 bits of a plain text block is treated as 16 bytes. These 16 bytes are used as a matrix by placing them in 4 rows and 4 columns. This is used for simplification. The encryption process consists of rounds and each round has 4 processes:

(I) Byte substitution
(ii) Shift rows
(iii) Mix Columns
(iv) AddRoundKey

For decryption the above mentioned 4 processes are conducted in the opposite (reverse) order.

In Proposed hybrid algorithm first SPK algorithm is applied and file is converted into strings and then strings into bytes, which are later taken compliment as encryption process. Once this is done, the newly obtained cipher is now passed as input to AES encryption. This covers up the main purpose of the project as, to secure the data, now the decryption key is sent to user mails using SMTP (Simple Mail Transfer Protocol) which provides additional security within the network.

March - April 2020
ISSN: 0193-4120 Page No. 11480 - 11487



Algorithm Used

1) File is Uploaded to Database by any user or admin
2) File Encryption is done with combined algorithm of SPK and AES Encryption as-
i) File is taken as strings of data.
ii) Every word in file is converted to its ASCII value.
iii) Now ASCII values are replaced by their binary values.
iv) Compliment is taken of the binary value,giving as the input data for AES algorithm.
v) Standard AES-256 algorithm is used to encrypt this newly obtained data.
vi) Cipher obtained now is the file made available for download to each user.
3) Decryption Password is send to user registered Email within organisation.
4) While opening the file if the password entered is right, Decryption begins as
i) Standard AES-256 decryption is done which gives us the complimented binary values.
ii) Now the compliment of the binary values is taken which returns original file binary values.
iii) binary values are converted into relative ASCII values which becomes the original file.
5) Admin portal records every download of file from each user to identify if anyone discloses the data.

4. Results Discussion

The research work on the project is done using the accurate techniques and with proper time management. As the project has come into working condition, it will be really helpful since we will be able to monitor the files and documents as well as protect them using encryption key all the while taking necessary precautions to avoid data leakage. Organizations can remain more aware about the negative or unwanted activities or actions and can prepare themselves beforehand. As the systems keep track of all the users - authorized and unauthorized, limiting the access to files on a need to know basis as decided by the admin, it reduces significantly the chance of any intervention from the outside. Also, if the system is deployed in a closed environment such as the company server or on the cloud only accessible from certain systems, it will be very easy to monitor and intrusion from the outside as well as inside.

5. Conclusion

The proposed system while capable of encrypting a document and making it only available to certain authorized users is still quite vulnerable to Logon-abuse attacks. Future implementation can be done by using Artificial Intelligence to create an intrusion detection system that is capable of monitoring a system for malicious activity such as multiple downloads of the same file by a user or multiple violations such as sharing of the files to unauthorized user and self-adapting in a way to block these attempts. In case of repeated transmission or requests to download within a set amount of time, the server can put a flag on the transmissions. It continues to check the transmissions. After one such occurrence a warning may be displayed. If this happens more than three times then the server terminates the user authorization and suspends the account.

References

[1] The Importance of Understanding Encryption in Cybersecurity – FloridaTech. [Online] http:// https://www.floridatechonline.com/blog/information-technology/theimportance-of-understanding-encryption-in-cybersecurity/

[2] Symmetric vs. Asymmetric Encryption. [Online] https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-whatare-differences

[3] Tutorials point – Advanced Encryption Standards. [Online] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard. htm

[4] Tutorials point – Data Encryption Standards, [Online] https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm

[5] WolframMathWorld – RSA Encryption. [Online] http://mathworld.wolfram.com/RSAEncryption.html

[6] G.Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of

Computer Applications, vol.67, no.19, pp.33-38, 2013.

[7] P.Patil, P. Narayankar, D.G. Narayan and S.M Meena ,"A Comprehensive Evaluation of Cryptographic Algorithms: DES,3DES, AES, RSA and Blowfish", Procedia Computer Science, vol.78,pp.617-624, 2016.

[8] B.Nithya and P Sripriya, "A Review of Cryptographic Algorithms in Network Security", International Journal of Engineering and Technology, vol.8, no.1, pp.324-331, 2016.

[9] N. Priya and M. Kannan, "Comparative Study of RSA and Probabilistic Encryption/Decryption Algorithms –

[10] Cryptography Algorithms: A Review - Anjula Gupta, Navpreet Kaur Walia.

[11] N.Singhal and J.P.S.Raina, "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, pp.177-181, 2011.

[12] T.Al-Somani and K.Al-Zamil, "Performance Evaluation of Three Encryption/Decryption Algorithms on the SunOS and Linux Operating Systems", 2011.

[13] R.S. Dhakar, A.K. Gupta and P. Sharma "Modified RSA Encryption Algorithm (MREA)", in Proc. of the Advanced Computing & Communication Technologies, 2012.

[14] M. B.Yassein, S.Aljawarneh, E.Qawasmeh, W.Mardini and Y.Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms", in Proc of the International Conference on Engineering and Technology, 2017.