[1] Jeethu Mathew

[2] Jemima Priyadarsini R.

Efficient DDOS Prevention in Internet of Medical Things Using 2aes and Digital Signature Approaches

Journal of Electrical Systems

Abstract: - All significant software and hardware systems require network security to operate properly. Organizational management and administration are essential to provide software and hardware protection. The secrecy of the data is another crucial factor. Network security relies heavily on cryptography to guard against unauthorized access. Confidentiality No third party will be able to evaluate or examine the supplied data. The use of encryption has overcome the problem over the long term. Only when applying cryptography, a set of techniques executed with the use of secured secret keys that transform the original communication into an encrypted message and vice versa, can the true sender and recipient of the information access the information. The algorithm in computer networks consists of a collection of compound mathematical formulas which represent the rules in the conversion of cipher text to plain text and vice versa along with the assured key. Particularly for controlling access to digital and physical resources including rooms, buildings, and computing equipment, biometric authentication methods are employed. The method of biometric identification uses biometrics, such as fingerprints or retinal scans, to identify a person. Biometric authentication makes use of biometric data to confirm a person's identity. Improving data security while executing encryption and decryption operation is the main issue that's to be addressed in this research. The main goal of the research is to provide a novel algorithm that, by minimising a significant range of time delays necessary to maintain the integrity of the information, boosts security while improving performance. In this research medical data in medical IoT has been encrypted and decrypted to secure the data from DDOS attack. Algorithms such as 2AES, 2RSA, 2DES, 2Blowfish along with Digital Signature is done in this research. Various metrics like Time Complexity, Space Complexity and Retrieval Time have been analyzed. From the results it's proved that 2AES with Digital Signature provides better results than other algorithms. The tool used for execution is Python.

Keywords: Healthcare, DDoS, Network Security, AES, DES, RSA, Time Complexity, Space Complexity, Retrieval Time.

I. INTRODUCTION

The physical component of information security is thought to be network security. It is crucial to have safe information transmission alongside networks and computers. The insertion of a variable by the cipher as a component of the created algorithm makes the procedure effective. The included variable is referred to as a key, which ensures that the cipher's output is distinctive. The type of cipher that the sender used to encrypt the data and the key used as variables must both be predicted by the intruder when they intercept the encrypted message. The process of encryption is a useful security strategy due to the time needed and difficulties in anticipating the specifics of information theft. For a long time, encryption has been the protective way for sensitive information. Classically, encryption was utilized by governments and militaries.

Data When it comes to the security of data, encryption becomes a crucial process. Data must be encrypted before being transferred across a network, and once there, the received data must be decrypted in order to reveal the original data. There are currently several sophisticated encryption methods available, and they are all easily vulnerable to an outsider's attack. When ciphertext is used for encryption, the most frequent attack is a brute force attack, in which the attacker tries all possible combinations of keys to decrypt the data.

The operator must choose the sort of cipher that will best identify the message's true meaning at the beginning of the encryption process. They must also list the variables that will serve as the message's unique encryption key. Some of the most used cipher types fall under the symmetric and asymmetric categories.

[1] Research Scholar, Department of Computer Science, Bishop Heber College Trichy, Affiliated to Bharathidasan University Trichy.

Email: jithumap@gmail.com

[2,] Associate Professor, Department of Computer Science, Bishop Heber College Trichy, Affiliated to Bharathidasan University Trichy.

Email: jemititus@gmail.com

Symmetric ciphers, which use a single key, are also known as secret key encryption. Since the computing system or sender who performs the encryption must share the private, enhanced key with all parties authorised to decrypt the information, the key used in the process is referred to as a shared secret.

Strictly speaking, symmetric key encryption operates significantly more quickly than asymmetric encryption. AES, which was developed to protect government-classified data, is one of the most widely used symmetric-key ciphers.

Asymmetric ciphers, often known as public key encryption, use two different yet conceptually related keys. Due to the computational difficulty of accounting for the huge prime numbers and reverse-designing the encryption, this type of cryptography frequently uses prime numbers to generate keys. The RSA encryption algorithm is the most often used public key algorithm. The information will be encrypted using RSA using either the private or public key; however, if the key is not used for encryption, it becomes a decryption key.

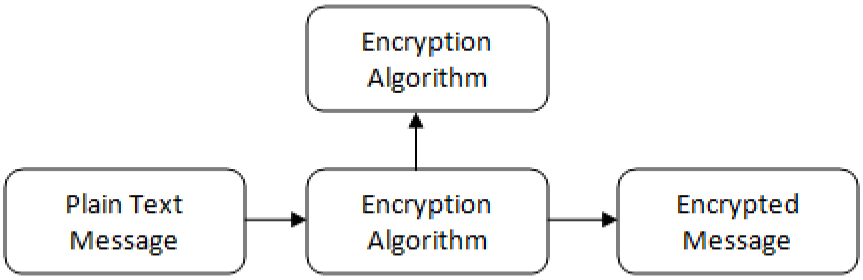

Figure 1: Encryption Process

The remaining portions of this work are structured as follows: The surveys made in detail that are relevant to DDOS prevention are covered in Section 2. The various models used in this research is described in Section 3. Detailed proposed methodology is given Section 4. The experimental results of the suggested algorithm on two different types of datasets will be shown in Section 5; the study's conclusions will be presented in Section 6.

II. Literature Review

Data encryption and decryption are dependent on secret keys that help with different techniques in cryptography. Based on the services of security, Vinaya Kulkarni et al., (2020) advised network security. The structure and use of network security approaches are described in detail in the study. The amount of data resources that today's society uses enhances the need for security. Some of these apps' security is achieved via cryptographic techniques like DES. However, there are several flaws in the current algorithms that must be fixed. In order to secure the confidentiality and privacy of data, new algorithm mechanisms are now the focus of study in the domains of networks and data security.

Due to the networking dangers, it is imperative to take action to safeguard both the network and computer security, which is a crucial concern. The systems are also impacted by problems brought on by harmful hubs. The system uses the resources from different hubs and looks after the resources. An overview of network security and the many methods used to improve network security, such as encryption, was provided by Sandeep Tayalo et al., (2018). The sensitive interaction between a system, the internet, and information security has resulted in an unavoidable sensitivity to any connection between an internal private system and the internet. Over time, data security becomes incredibly important.

The network provider's main concern is the security of the client's personal information. The study demonstrates various plans utilised as a component of cryptography to achieve network security goals. A fundamental strategy for obtaining the robust security from the cloud is to encrypt messages with strong security keys that can only be learned through communication with the recipient and beneficiary side. The safe exchange of the key is a crucial task between the information sender and recipient. The categorization of mysterious data received from unauthorised clients is delayed by the key administration. The traded message's veracity will be examined using checking of respectability.

Implementing cryptographic calculations in system applications and system norms is a necessary step in security arrangement. The study focuses on the threat posed to PC system security and swiftly illustrates the concept of PC security. The key administration, key distribution, and optimum cryptography formulation for mist-based information security should all be made achievable.

The networks used for information exchange are public when data is transferred outside the enterprise and private when data is transferred within the company. In many different kinds of institutions, organisations, and businesses, network security is carried out. Mukund R. Joshi & Renuka Avinash Karkade (2015) performed research on the fundamentals of cryptography and how it is used. The study describes the cipher-based cryptography systems. It describes many cryptography models and algorithms. By enacting restrictions and limiting access for unauthorised users with the aid of resources that are accessible across the network, the network administrator safeguards the information. Additionally, the administrator must routinely measure and check on the efficiency of the network security provided. By thoroughly examining all of the different cryptography algorithms, the research's primary goal is to improve network security effectiveness. When cryptography is used in conjunction with an appropriate communication protocol, digital communication is highly protected against hacker attacks while taking into account communication between two distinct computers.

Huaqing Lin et al., (2018) investigated and clarified network security statistics. Data analysis makes it possible to identify network breaches and attacks, which opens up the potential of assessing the security level for the entire network system at a higher level. The first step in foreseeing network risks and breaches is to collect security-related data. In any case, the setting of 5G and big data has increased the difficulties in gathering data linked to network security. The study collects information about security, including its synonyms and traits. Additionally, the area where network data will be applied is gathered. The research then outlines the purpose and specifications for the gathering of security-related data and frames a taxonomy model for the existing data collection methods. To achieve high quality in the collection of security-based data, a study of the existing collection methods, collection processes, and collection nodes based on network data gathering was conducted, and the data were examined in relation to the suggested objectives and requirements. The study highlights how crucial it is to research network security-based data collection for identifying network breaches and attacks. The mechanism for best utilising the security data is aided by the data collection method-related taxonomy that is offered in the research. Additionally, a briefing on the research's current problems and problems was given. The research was completed with improved understanding when the open research issues were finally discussed.

Jingjing Hu et al., (2020) demonstrated both the network and the host can be used to measure the risk associated with network security. Additionally, it suggests a brand-new framework for a multidimensional assessment method that entails two steps—risk calculation and risk identification—to identify network security risks. The research suggests a mechanism for a multidimensional hierarchical index that evaluates the risk related to cyber security at the risk identification stage. The three different elements of the security system's status—vulnerabilities, threats, and fundamental functionality—are what direct the data collection process.

It is impossible to sort out the characteristics of the internal network assault using security metrics research on attack graphs. So Chun Shan et al., (2018) suggested an attack probability-based internal security metric system for networks. The suggested method offers a number of advantages, including a tracking event node that simplifies the attack graph method and offers a countermeasure to the attack graph's exponential expansion along with the network's size. Additionally, it helps to undermine covert internal attacks and improves the effectiveness of the entire system. The advantages include the ability to more easily calculate the likelihood of an assault strategy based on a streamlined attack graph that makes the strength of internal defences more clear.

The findings demonstrate that the attack probability-based internal network security metric approach resolves problems with the current metric approaches for the effective maintenance of security when implementing the attack graph devoid of the internal network. Using a relationship between the temporal differences and viewing the event node, the attack graph is condensed. The method recommends the assessment method of cumulative reachable probability to various types of target nodes gathered from vulnerabilities with the indications of CVSS metric along with directed edges relationship. It also puts forth the methodology of key-value pair to inspect the attack graph. The simulation results show that the attack graph simplification strategy has a substantial impact on increasing efficiency.

Currently, digitalization is a key factor in how seamlessly each person's life is integrated with digital technologies. Shruthi Prabhakar et al., (2017) proposed a number of strategies for fending off attacks as well as a number of countermeasures. Numerous software programmers exist to help identify assaults and safeguard the network, but manual intervention is still more effective in stopping attacks. The research provides numerous straightforward approaches that can be used to readily thwart various threats. Researchers throughout the world are compelled to design a new strategy to secure the data from these attacks as the current attacks change and get more complex. In the network area, many elevations are being framed.

A defensive approach was put up by Donglan Liu et al., (2019) to guard against vulnerabilities brought on by virus or hacker attacks on computer data. Researchers have developed a variety of techniques to identify and prevent network assaults. The paper investigates network problems and attack detection methods based on reverse detection and protocol analysis. the power system's big data environment, where the attack packets are restarted and iterated for speedy detection and diagnosis of the network assault, is continuously monitoring the network attack packets. The results of the experiments show that the suggested method successfully locates the assault in the network and conducts a thorough study of the attack process. Additionally, it pinpoints the attack's unique behaviour as well as its course.

People are now more aware of the importance of network security thanks to the internet's and computer networks' rapid expansion. Network security is the key problem in computing since attack types are changing and becoming more diverse every day. The mobile ad-hoc network is not dependent on any specific nodes. The protection of the computer system and the information is the most important aspect of network security. The malicious nodes cause a network barrier to form. These selfish nodes are malevolent because they use the resources of other nodes while still protecting their own resources. After evaluating and quantifying the integrity, accessibility, and confidentiality aspects of network data security by Mohan Robbi et al., (2015). They are network security confidentiality vector, network security availability vector, and network security integrity vector.

Depending on how difficult it is to crack them, different algorithms provide varying levels of protection. The most popular hashing algorithms include MD5, MD4, SHA, and others. The research conducted by Arvind K. Sharma et al., (2019) provides evidence of the importance of hash functions. The compression functions and hash functions are frequently employed in networking, with the latter focusing more on attacks when appropriate.

I. Sumantra and Dr. S. Indira Gandhi et al., (2020) developed a successful project to identify and counteract DDoS attacks in the SDN. Distributed Denial of Service assaults are among the most harmful in the online world. When a website is likely the target of a DDoS assault, it has been compromised. A DDoS attack's primary goal is to disrupt the computer system's normal operation by denying legitimate users access to resources and services by flooding the network with an excessive amount of unnecessary traffic from a distributed source. Botnet refers to the dispersed collection of hosts that produce threats.

A new method called the SAD technique was suggested by J. Vijitha Ananthi and S. Vengatesan (2017) to prevent security. The proposed method is utilised to identify the DoS attack types in wireless ad hoc networks. The method uses four different kinds of attack detection. In most cases, identifying the sort of malicious assault is more important than identifying a rogue node. The SAD methodology can identify wormhole, botnet, sinkhole, and black hole attacks. Any intermediate node blocking the flow of data to the target results in a black hole attack. Wormhole attacks happen whenever an attacker node disturbs the adjacent nodes. When a certain node exerts an overflow, a botnet attack occurs.

II. Materials And Methods

2DES

As it cannot survive attacks, DES is seen as being insecure. DES is employed to encrypt electronic data. Data privacy and authentication are the two fundamental tenets of contemporary data encryption. Data Encoding Protocol (DES), a block cipher that was launched in 1997 and for which NIST presented the first cipher standard, commonly abbreviated as DES. The DES approach's block size and main size are both 64 bits, making them symmetrical algorithms. A 64-bit plain text is sent to the DES algorithm, which returns a 64-bit ciphertext as a result. Information is encoded and decoded using essentially the same type of key and code. 2DES means the DES is performed twice.

2Blowfish

The forementioned technique was created in 1993 by Bruce Schneier and is still widely utilised today. In this way, a 32-448-bit variable duration key is used to encode 64-bit binary clocks. The strategy has shown to be incredibly resilient because no attack has yet been successful against it. The procedure is time-consuming and energy-intensive. For systems like packet switching where keys occasionally change, the blowfish block's height of 64 levels is inappropriate. This method works well for systems when the key is not updated regularly. 2Blowfish means the Blowfish is performed twice.

2AES

An Enhanced Encryption Standard is AES. It is one of the replacements for DES that NIST has proposed. The only assault that successfully cracks the code is one that uses brute force. The hackers will use every possible character combination to attempt to break the encryption during this attack. AES is also a block cipher, much like DES. This approach employs keys with lengths of 256, 192, or 128 bits. Depending on the size of the switch, the 128-bit data blocks are encoded in different sizes such 14, 12, and 10. The algorithm has advantages in terms of simplicity, scalability, and platform compatibility. 2AES means the AES is performed twice.

2RSA

In 1977, Rivest, Leonard Adleman, and Adi Shamir created the RSA computer. With this method, a private key remains with the client and will not be shared with anybody, but an open key is given to anyone who will use it to scramble the information that needs to be communicated. Figure content and plain content are both widely whole numbers in this evaluation, ranging from zero to n-1 for the same n. The achieved equation C= Me mod n is used to encrypt the plain text into blocks. Here, C denotes the content of the figure, while M is the plain content. Similar to how the implied equation M= Cd mod n, where d stands for the simple content is taken for the private key. 2RSA means the RSA is performed twice.

Digital Signature

A random signature value K that is undisclosed, recognizable, and in a chunk has been assigned for the DSA method. If some bits of K are compressed, the signature should be created in such a way that the attacker cannot simply use the same value of K numerous times to discover the attacker's private key.

III. Proposed Methodology

DIGITAL SIGNATURES (DS)

During data transfer, several encryption techniques are employed to authenticate messages. In the actual world, signatures are typically written by hand or on a computer. DS is a style of strategy that connects users to digital-style material. People from the destination area and the other authenticated intermediary layer individuals may confirm linking. The secret key value and data that the sender has identified are used to calculate the encrypted value known as DS. The recipient of the message frequently demands authenticity, or proof that the sender is the rightful owner of the particular content.

The security method known as DS allows the sender to include the code that is used as the signature value. The signature information is altered to sign and modify based on the relevant message information. The receiver receives DS along with the original message. DS enables the message's recipient to validate the data obtained and validate the information received. As a result, the public key value DS offers authentication and data integrity services. Additionally, it provides non-repudiation services.

Pseudo code of Two Factor AES with DS Authentication:

In this research work, the dataset is protected by 2AES with DS. The encryption process is executed using 2AES algorithms and the decryption process is handled using DS. The following steps illustrate the working procedure of the data encryption using 2AES and DS.

Signature Key Length = (Received signature key Length value)/(Actual signature key Length Value)- - - -(1)

```
Step 1: Start
Step 2: Load initial n-dimensional dataset
Step 3: Assume dataset size k;
Step 4: Now divide dataset into single blocks.
Step 5: Now this single block will be divided into sub blocks with equal bit allocation.
Step 6: Assume K1and K2 as two different keys
Step 7: Now encrypt the dataset with a single AES with key K1
Step 8: Now encrypt the dataset with a single AES with key K2
Step 9: Now use Digital Signature for authentication
Step 10: Calculate Digital Signature Key length
Step 11: If (Signature Key Length=Received Signature Key Length);
Step 12: Choose the correct file
Step 34: Else if (Signature Key Length=Received Signature Key Length);
Step 14: Do not choose file and Repeat step 10 again
Step 15: Now decrypt the dataset with a single AES with key K1
Step 16: Now decrypt the dataset with a single AES with key K2
Step 17: Stop
```

Architecture of Two Factor AES with DS Authentication:

Nowadays, most researchers propose various encoding and decoding approaches like DES, RSA, AES, and others. Even though the existing methods can protect the information from attacks, they are unable to withstand the revised and upgraded style of threats. This gap is mandatory to satisfy the security in information transmission. The most popular problems encountered in algorithms are a shortfall in reliability and a significant amount of time that need to be included in the packet delay to sustain the security in the channel of communication among the terminals. Figure 2 below demonstrates the Architecture of 2AES and DS Authentication techniques.

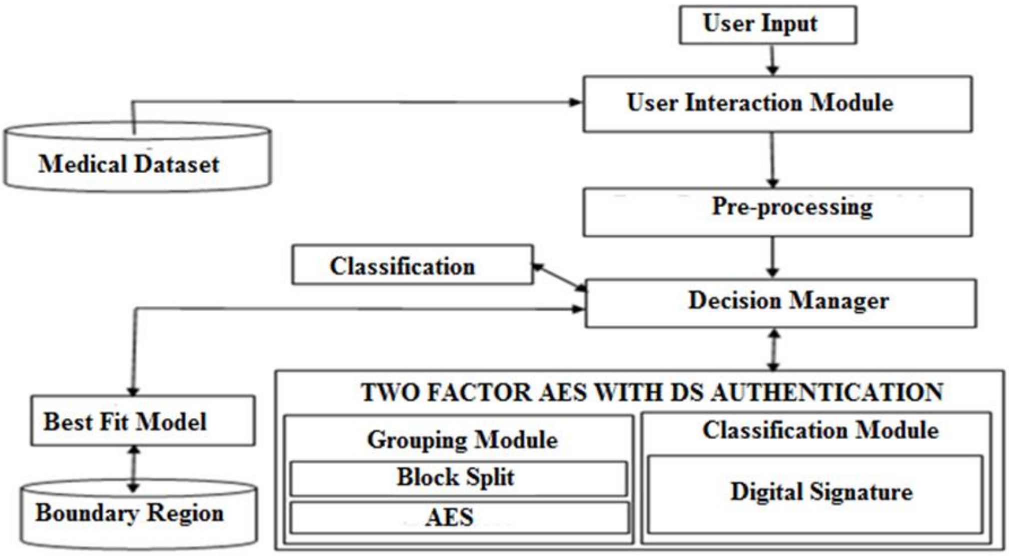

Fig.2 Architecture of Two Factor AES with DS Authentication

Dataset Description

Datasets used for DDOS detection is Chronic Kidney Disease (CKD) and Pima Indians Diabetes (PID) dataset which is downloaded from kaggle.com. The suggested algorithm's performance is assessed using the two types of datasets listed below.

Chronic Kidney Disease (CKD) Dataset: Here is the dataset collected from CKD (Chronic Kidney Disease) dataset. It contains 400 instances. It is been downloaded from online source provider called Kaggle.com. Totally 26 numerical parameters such as Id, Blood Pressure, Glucose, Insulin, Age, BMI level are denoted for every patient in the given dataset.

Pima Indians Diabetes (PID) Dataset: Here is the dataset collected from PID (Pima Indians Diabetes) dataset. It contains 9 instances. It is been downloaded from online source provider called Kaggle.com. Totally 9 numerical parameters such as Pregnancies, Blood Pressure, Glucose, Insulin, Age, BMI level are denoted for every patient in the given dataset.

IV. Results And Discussion

Two well-known datasets termed Chronic Kidney Disease (CKD) and Pima Indians Diabetes (PID) dataset are used in a series of tests and analyses to assess the performance of the suggested methodology. Various metrics like Time Complexity, Space Complexity and Retrieval Time have been analyzed. The formulas of metrics used are given below:

Time Complexity:

$$P_1(n)\,T_1(n)+P_2(n)\,T_2(n)+P_3(n)\,T_3(n) \tag{2}$$

Here $T_1(n), T_2(n), T_3(n)\ldots$ represents the execution time.
$P_1(n), P_2(n), P_3(n)\ldots.$ indicates the input probability values.

Average Time Complexity:

$$T(n)= I/(D\ )+ \text{Biometric Process Time} \tag{3}$$

Here I denotes the total input file or text file
D Indicates distributed size of each block

Average Space Complexity:

$$\text{Average Space Complexity}=\text{Temp.space}+\text{Input\_Space} \tag{4}$$

Here Temp.Space denotes Temporary Space
Input_Space denotes Space occupied by Input File

Retrieval Time:

$$\text{RTime}=\text{Total File Size}/\text{Average Time Complexity} \tag{5}$$

Here RTime denotes Retrieval Time
Total File Size denotes the actual size of the Input File
Average Time Complexity denotes the overall time consumed by each algorithm.

1. Chronic Kidney Disease (CKD) Dataset Analysis:

Time Complexity Comparison:

The following Table 1 and Figure 3 represent the Time Complexity comparison of 2RSA, 2DES, 2Blowfish and 2AES with Digital Signature authentication. From the result it is proved that 2AES+DS work better than other algorithms.

Table.1 Time Complexity Comparison

Iterations of Patients Record (Bytes/sec)	**2RSA+DS (msec)**	**2DES+DS (msec)**	**2Blowfish+DS (msec)**	**2AES+DS (msec)**
10	28	34	29	26
20	55	60	57	52
30	62	68	62	60
40	67	75	67	65
50	74	74	74	73

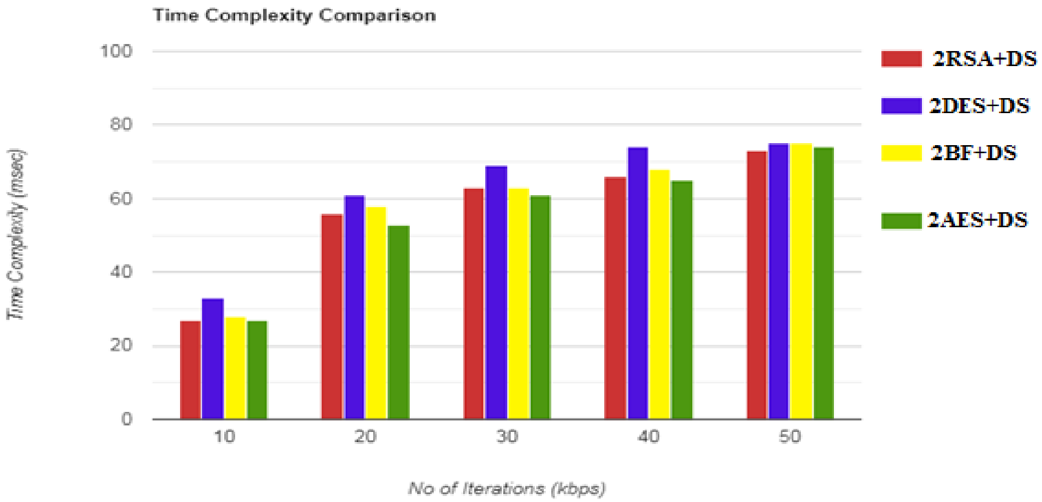

Fig.3 Time Complexity Comparison Graph

Average Time complexity Comparison:

The following Table 2 and Figure 4 represent the Average Time Complexity comparison of 2RSA, 2DES, 2Blowfish and 2AES with Digital Signature authentication. From the result it is proved that 2AES+DS work better than other algorithms.

Table.2 Average Time complexity Comparison

Algorithms	**Average Time Complexity (msec)**
2RSA+DS	62.2
2DES+DS	65.1
2Blowfish+DS	56.5
2AES+DS	54.3

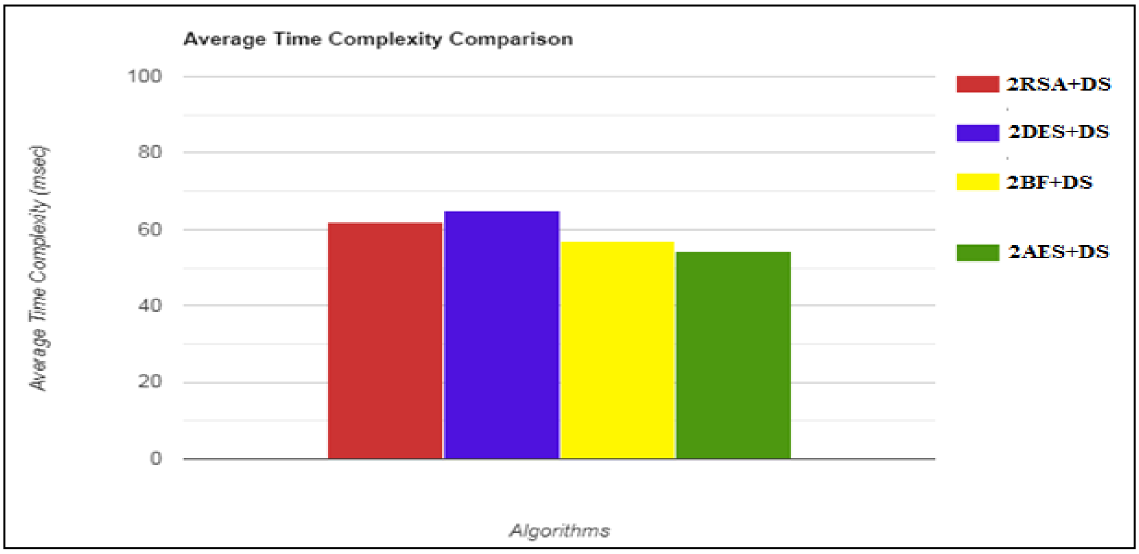

Fig.4 Average Time Complexity Comparison Graph

Average Space Complexity Comparison:

The following Table 3 and Figure 5 represent the Average Space Complexity comparison of 2RSA, 2DES, 2Blowfish and 2AES with Digital Signature authentication. From the result it is proved that 2AES+DS work better than other algorithms.

Table.3 Average Space Complexity

Algorithms	Average Space Complexity (Bytes/sec)
2RSA+DS	2977
2DES+DS	3288
2Blowfish+DS	2928
2AES+DS	2848

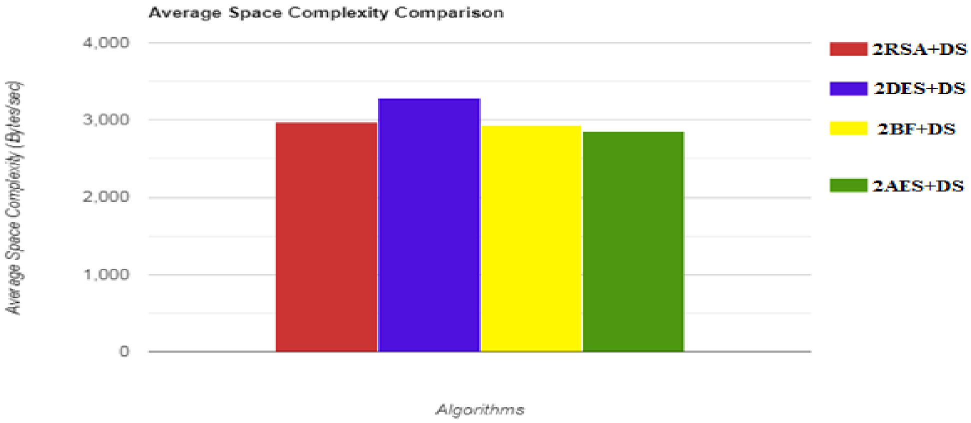

Fig.5 Average Space Complexity Comparison Graph

Retrieval Time Comparison:

The following Table 4 and Figure 6 represent the Retrieval comparison of 2RSA, 2DES, 2Blowfish and 2AES with Digital Signature authentication. From the result it is proved that 2AES+DS work better than other algorithms.

Table.4 Retrieval Time Comparison

Algorithms	Retrieval Time (msec)
2RSA+DS	86
2DES+DS	90.5
2Blowfish+DS	86
2AES+DS	85.4

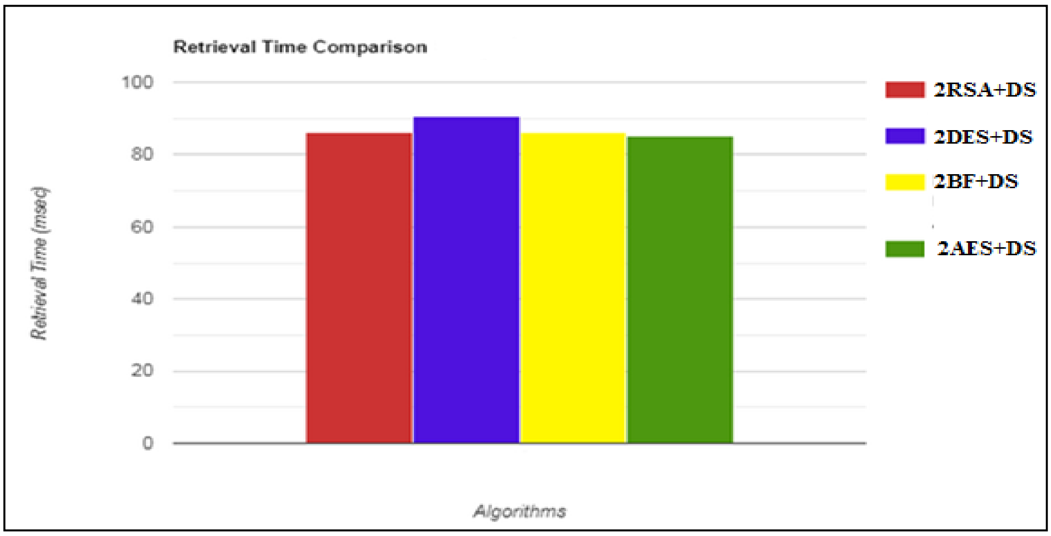

Fig.6 Retrieval Time Comparison Graph

2. Pima Indians Diabetes (PID) Dataset Analysis:

Time Complexity Comparison:

The following Table 5 and Figure 7 represent the Time Complexity comparison of 2RSA, 2DES, 2Blowfish and 2AES with Digital Signature authentication. From the result it is proved that 2AES+DS work better than other algorithms.

Table.5 Time Complexity Comparison

Iterations of Patients Record (Bytes/sec)	2RSA+DS (msec)	2DES+DS (msec)	2Blowfish+DS (msec)	2AES+DS (msec)
10	31	37	29	26
20	58	59	52	48
30	68	72	65	62
40	72	78	67	62
50	78	85	78	71

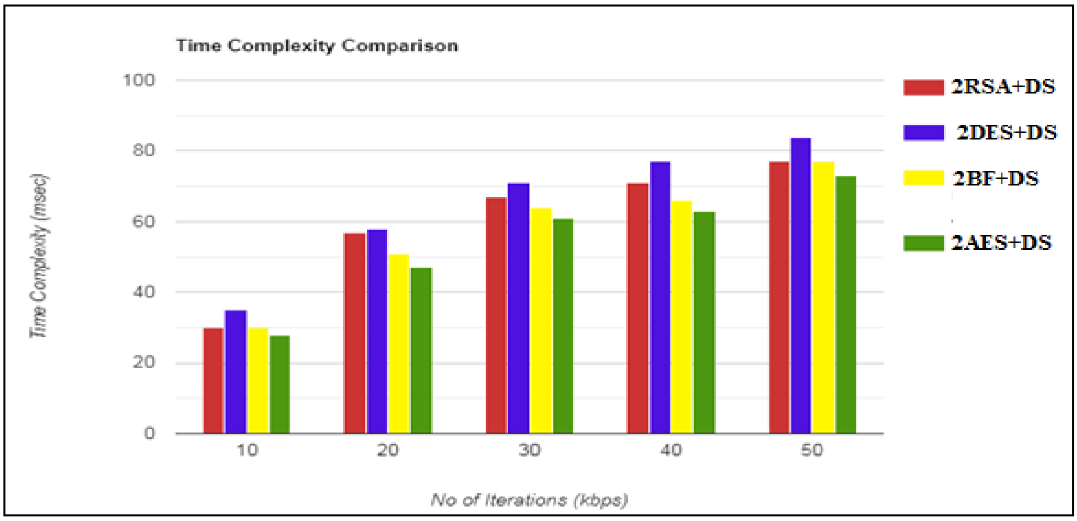

Fig.7 Time Complexity Comparison Graph

Average Time complexity Comparison:

The following Table 6 and Figure 8 represent the Average Time Complexity comparison of 2RSA, 2DES, 2Blowfish and 2AES with Digital Signature authentication. From the result it is proved that 2AES+DS work better than other algorithms.

Table 6: Average Time complexity

Algorithms	Average Time Complexity (msec)
2RSA+DS	64.6
2DES+DS	66.8
2Blowfish+DS	63.5
2AES+DS	60.9

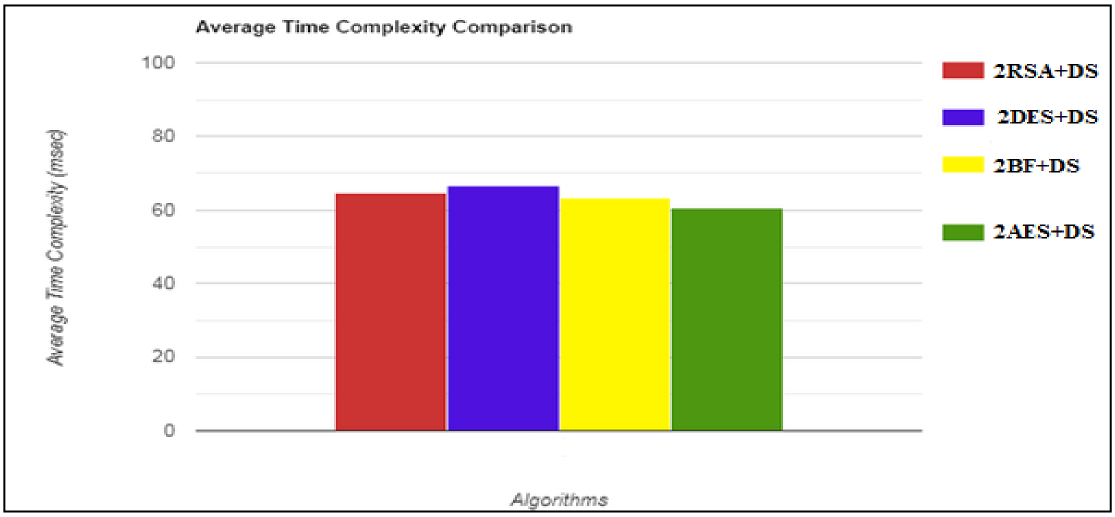

Fig.8 Average Time Complexity Comparison Graph

Average Space Complexity Comparison:

The following Table 7 and Figure 9 represent the Average Space Complexity comparison of 2RSA, 2DES, 2Blowfish and 2AES with Digital Signature authentication. From the result it is proved that 2AES+DS work better than other algorithms.

Table.7 Average Space Complexity Comparison

Algorithms	Average Space Complexity (Bytes/sec)
2RSA+DS	3375
2DES+DS	3405
2Blowfish+DS	3375
2AES+DS	3278

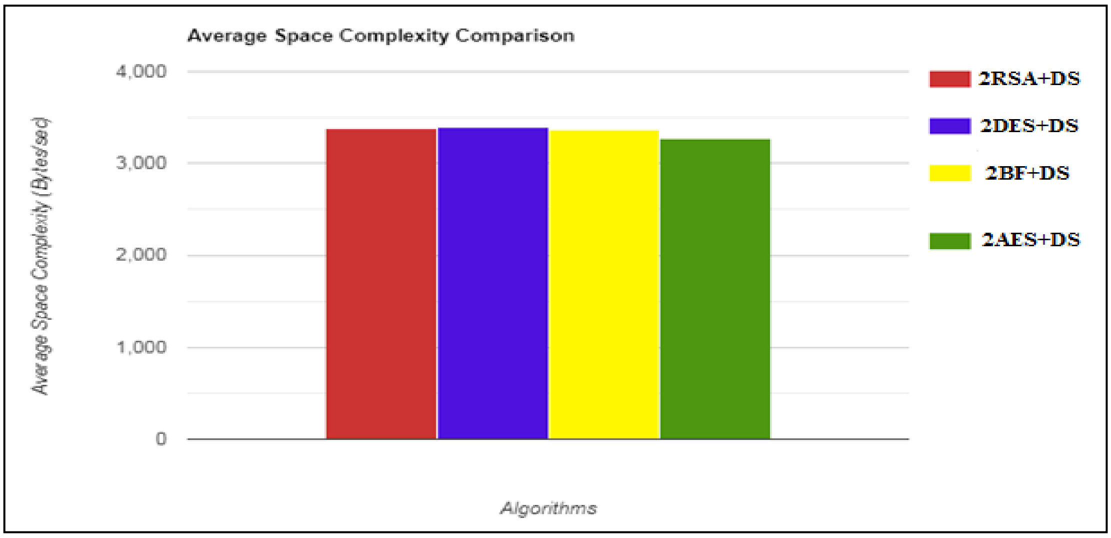

Figure 9: Average Space Complexity Comparison Graph

Retrieval Time Comparison:

The following Table 8 and Figure 10 represent the Retrieval comparison of 2RSA, 2DES, 2Blowfish and 2AES with Digital Signature authentication. From the result it is proved that 2AES+DS work better than other algorithms.

Table.8 Retrieval Time Comparison

Algorithms	Retrieval Time (msec)
2RSA+DS	93.1
2DES+DS	95.2
2Blowfish+DS	89.7
2AES+DS	87.4

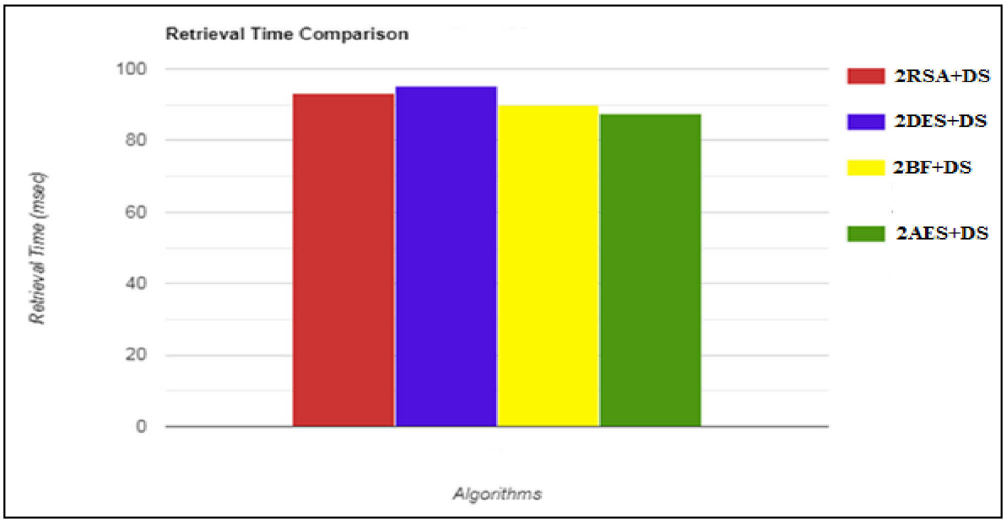

Fig.10 Retrieval Time Comparison Graph

V. Conclusion

Network security is the most important element of information security since it is responsible for safeguarding all information that moves via computer networks. The provision to build a foundational network infrastructure for the computers is part of network security. Only those with the proper authorization can access data thanks to cryptography, which encrypts the data. Using the encryption algorithm, a user message or piece of information that is in plain text is transferred. Several different techniques are currently available to securely transform or encrypt the data. The well-known network security algorithms 2DES, 2AES, 2AES and 2Blowfish are only a few examples. However, hackers are powerful enough to access and alter private data, endangering its confidentiality. Being dishonest, an invader focuses especially on stealing crucial identities or data. The user is put in a dangerous environment as a result. In order to improve security in an open network, the current procedures must be upgraded further. The encryption techniques convert essential information into secret codes to hide the real meaning of the information. Therefore, cryptography is considered as the science of encryption and decryption of information. According to computing, the unencrypted raw data is called plain text, and the encrypted data is known as ciphertext. The complex formulas used for encoding and decoding the messages are known as encryption algorithms or the ciphers. To conceal the material's true meaning, encryption techniques transform crucial information into secret codes. As a result, the science of information encryption and decryption is known as cryptography. In this research medical data in medical IoT has been encrypted and decrypted to secure the data from DDOS attack. Algorithms such as 2AES, 2RSA, 2DES, 2Blowfish along with Digital Signature is done in this research. Various metrics like Time Complexity, Space Complexity and Retrieval Time have been analysed. From the results it’s proved that 2AES with Digital Signature provides better results than other algorithms. The tool used for execution is Python.

VI. References

[1] Vinaya Kulkarni, ShivaliKirdat, Sneha Patil & C.H.Patil (2020),” Study on Network Security Algorithm”, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 20 Conference Proceedings, Kattankulathur, India, Vol. 8, No. 05, pp. 1-3.

[2] Sandeep Tayal, Nipin Gupta, Pankaj Gupta, Deepak Goyal & Monika Goyal (2017), “A Review paper on Network Security and Cryptography”, Advances in Computational Sciences and Technology, ISSN 0973-6107, Vol. 10, No. 5 pp. 763-770, Research India Publications.

[3] Mukund R. Joshi & RenukaAvinash Karkade (2015),"Network Security with Cryptography", ISSN 2320–088X, International Journal of Computer Science and Mobile Computing, Vol. 4, Issue. 1, January 2015, pp. .201 – 204.

[4] Huaqing Lin, Zheng Yan, Yu Chen & Lifang Zhang (2018), "A Survey on Network Security-Related Data Collection Technologies", IEEE Access Special Section On Internet-Of-Things (IoT) Big Data Trust Management, Vol. 6, pp.18345 – 18365.

[5] Jingjing Hu, Shuangshuang Guo, XiaohuiKuang, Fankun Meng, Dongsheng Hu, & ZhiyuShi (2020),” I-HMM-Based Multidimensional Network Security Risk Assessment”, IEEE Access Special Section On Distributed Computing Infrastructure For Cyber-Physical Systems, Vol.8, pp. 1431-1442.

[6] Chun Shan, Benfu Jiang, Jingfeng Xue, Fang Guan & Na Xiao(2018), "An Approach for Internal Network Security Metric Based on Attack Probability", Hindawi Security and Communication Networks Volume 2018, Article ID 3652170, https://doi.org/10.1155/2018/3652170, pp. 1-11.

[7] Shruthi Prabhakar (2017), “Network Security in Digitalization: Attacks and Defence”, International Journal of Research in Computer Applications and Robotics, ISSN 2320-7345, Vol.5, No. 5, pp. 46-52.

[8] Donglan Liu, Xin Liu, Hao Zhang, Wenting Wang, Xiaohong Zhao, Yang Zhao, Hao Yu & Lei Ma(2019), “Research on Network Attack Detection Technology based on Reverse Detection and Protocol Analysis “, IEEE 6th International Conference on Information Science and Control Engineering (ICISCE), 20-22 Dec. 2019, Shanghai, China pp. 490-494.

[9] Robbi Rahim, Andri Pranolo, Ronal Hadi, Rasyidah & Heri Nurdiyanto (2017), “Digital Signature Security in Data Communication”, Advances in Intelligent Systems Research (AISR), International Conference on Education and Technology, Vol 144, pp. 172-177.

[10] Arvind K. Sharma & S.K. Mittal (2019), “Cryptography & Network Security Hash Function Applications, Attacks and Advances: A Review“, IEEE Third International Conference on Inventive Systems and Control (ICISC), 10-11 Jan. 2019, Coimbatore, India, pp. 177-188.

[11] Sumantra .I & Indira Gandhi. S (2020), "DDoS attack Detection and Mitigation in Software-Defined Networks", IEEE International Conference on System, Computation, Automation, and Networking (ICSCAN),January 12, Chennai, India, pp. 1-5.

[12] Vijitha Ananthi. J & Vengatesan. S, (2017), “Detection of various attacks in wireless Adhoc networks and its performance analysis”,17th International Conference on Inventive Computing and Informatics (ICICI), 23-24 Nov. 2017, Coimbatore, India, pp. 754-757