

Analysis of Data Security Algorithm in Wireless Network

Girish Kumar Tiwari¹ Vikram Patel²

^{1,2}Department of Electronics & Communication Engineering

^{1,2}Ujjain Engineering College, Ujjain (M.P), India

Abstract— While using a smartphone, computer, or other device to transport data over a wireless network, data theft by unscrupulous parties is possible. The data may be accessed at any time and from any location. On the other side, data on the cloud is not necessarily secure. Because the end user can only access the data with the assistance of a third party. In such situation, we'll need to improve the security of our internet data transfer. It is impossible to stress the importance of ensuring security in wireless network cryptographic approaches. To increase the speed with which data is carried through a wireless network, algorithms are used. In this paper, We provide a new security method that combines symmetric and asymmetric cryptography techniques to give great security while requiring little maintenance. The performance of an algorithm for a network assault including one of the most popular network assaults and a range of input parameters was investigated and analysed using simulation. This study outlines a safe and efficient method for transferring data across wireless networks while retaining data integrity and confidentiality. To ensure authentication and data integrity, the suggested system integrates the ECC and the Advanced Encryption Standard (AES), Message Digest 5(MD5) technology. The results of the experiments reveal that the proposed strategy is effective and produces better outcomes than existing methods.

Keywords: TCL, C++, Elliptical curve cryptography (ECC), AES, MD-5, RC6, Wireless Network Security Algorithm

I. INTRODUCTION

Wireless communications network security algorithm refers to the information security of data and its important components, such as the software and hardware that process, store, and transfer it. In today's digital environment, cryptography is extremely crucial. To fulfil the diverse demands resulting from applications, several cryptographic algorithms have been created. A cypher, or cryptographic algorithm, is a mathematical function for encrypting and decrypting data. In general, there are two functions: one for encryption and the other for decryption. Encryption and decryption keep an adversary at a distance. getting information access The two computer languages used to convert regular text to encrypted text are Terminal command language (TCL) and C++. Other network simulation software pales in contrast.

Wireless sensor networks (WSNs) are particularly sensitive due to their broadcast nature and hazardous environment. As a result, there are a variety of solutions for security issues such as routing security. Safe key management and cryptography, as well as secure localization, are all important considerations. Cryptographic algorithms, which are a key part of wireless network security design, confront a variety of obstacles, including battery life and memory constraints. Due to these limitations, WSN is unable to deal with standard encryption schemes. With security algorithms, there are two fundamental difficulties. First, the amount of

data overload created in messages by security algorithms should be kept to a bare minimum; every bit matters.

To meet security needs such as Authentication, Confidentiality, and Integrity, a variety of cryptographic algorithms have been developed. Authentication refers to the process of stopping unauthorised users from accessing the network. Confidentiality refers to keeping information safe from prying eyes. Integrity assures the receiver that the data received has not been tampered with while in transit.

An adversary Data authentication can also be used to ensure data integrity. Encryption is the process of encrypting data in such a way that hackers cannot read it. The two types of encryption algorithms are asymmetric and symmetric encryption. Symmetric cryptography, often known as private-key cryptography, uses just one key to encrypt and decode data. Two popular symmetric encryption schemes are Data Encryption Standard (DES) and Advanced Encryption Standard (AES) (AES). Asymmetric key cryptography, often known as public-key cryptography, encrypts data using asymmetric keys.

And uses a set of keys to decode messages Elliptic Curve Cryptography (ECC) is a well-known asymmetric encryption technique (ECC). ECC is the foundation of both the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Elliptic Curve Diffie Hellman (ECDH) algorithms. There are advantages and disadvantages to both symmetric and asymmetric encryption algorithms.

The MD5 algorithm is a widely used cryptographic hash function that provides a 128-bit (16-byte) hash result. It has been utilised in a variety of security applications. This paper proposes and describes a hybrid cryptography approach. Its goal is to ensure the security of data and the trustworthiness of users. It requires working in two periods at the same time. In Phase I, it employs both AES and ECC algorithms to reap the benefits of a mix of symmetric and asymmetric cryptographic approaches.

The National Institute of Standards and Technology did not choose RC6 as the winner of an advanced encryption standard (AES) competition (NIST).

A. Attacks on wireless networks

Wireless network assaults, also known as wireless network penetration and intrusion attacks, pose a serious threat. Wireless network attacks are designed to gain access to the network.

The seven most common wireless network risks are as follows:

- 1) Common configuration errors include misconfigurations and incomplete settings.
- 2) Denial of Service (DoS). is the act of flooding a network with traffic (or viruses) in order to seize resources or establish backdoors.
- 3) Eavesdropping Passive capture is the practise of gathering sensitive information within range of an access point.

- 4) Rogue (or Unauthorized/Ad-Hoc) Access Points: To fool devices into connecting, create a fake access point.
- 5) Attacks by the Evil Twin: Using a louder signal to imitate legal access points in order to entice authorised users to sign on.
- 6) Obtaining access to lost or stolen wireless devices by circumventing the password.
- 7) Piggybacking. Freeloading can take the form of snooping on a connection or intercepting file sharing.

II. BACKGROUND AND PREVIOUS WORK

Researchers have spent a lot of time looking into the security of wireless communication networks. DES, 3DES, and AES are contrasted as encryption algorithms. The comparison is broken down into nine categories, such as ACSII printable character keys, the time it takes to check all potential keys (50 billion seconds), and so on. AES is more secure than DES and 3DES, according to these candidates. This study looks at a unique network security evaluation approach framework as well as a complete examination of the Multiple Attribute Decision Making (MADM) theory. This framework establishes a network security measurement paradigm by standardising the assessment technique. It also included step-by-step evaluation methods to ensure that the criteria were followed in practise. Following that, a network worm proliferation evaluation example is shown. When compare with to other techniques of evaluation, Their methods are more thorough and scientific, allowing them to rank each step of the worm life cycle and worm defence strategy in order of preference. The approach helps to standardise the network and conduct scientific study. a method for determining security A cryptographic algorithm (RC5) is also put to the test. The Blowfish and DES block cypher algorithms were compared using C# software. A comparison of RC5, Blowfish, and DES is done using a set of input files, and the encryption and decryption times are assessed. According to the findings, RC5 is 1.5 times quicker than Blowfish and 2.57 times faster than DES. They also discovered that the Blowfish method's performance is inversely related to key size, meaning that as the key size rises, so does its performance vice versa. Although all three algorithms utilise nearly the same amount of CPU, RC5 needs more RAM than Blowfish and DES in terms of resource use. As a result, the RC5 block cypher approach is more efficient and user-friendly than Blowfish. DES block cyphers algorithms. RC5 is an excellent choice when a high encryption rate is required.

ECC is a public key encryption method based on the algebraic structure of elliptic curves over finite fields. ECC enables for fewer keys to be used than non-EC encryption (based on simple Galios fields) and getting equal security. Elliptic curves can help with key agreement, digital signatures, pseudo-random generators, and other tasks. They may be utilized for encryption indirectly by combining the key agreement with a symmetric encryption method. Elliptic curves are also used in a number of elliptic curve-based integer factorization algorithms with cryptographic applications, where the provided plain text is encrypted first using AES and then with ECC. The hash value of this encrypted cypher text is calculated using the MD5 method. On the other hand, the Hash value is evaluated and integrated

first. The cypher text is then decrypted using the AES and ECC decryption algorithms. As a consequence, it is possible to derive the plaintext. This algorithm uses a combination of symmetric and asymmetric cryptography. This strategy, how takes a long time to perform because the plaintext is encrypted sequentially by both AES and ECC. With the same encryption and decryption structure, we provide an improved RC6 encryption algorithm. Until date, the encryption and decryption structures of standard RC6 methods were different. We created our strategy by introducing a symmetric layer using basic rotation and XOR operations, with half of the RC6 rounds encrypting and the other half decrypting. A symmetric layer sits between the encryption and decryption components. The suggested RC6 approach is nearly as quick as the existing RC6 algorithm. Nonetheless, including a symmetric layer into the proposed technique improves encryption security since assessing an encrypted stream using differential and linear analysis is difficult. The proposed technique will be advantageous for applications that require the same encryption and decryption procedure, such as light mobile devices and RFIDs.

First, we reviewed the foundations of earlier research papers, praised researchers' thoughts, and discussed the performance of several symmetric algorithms. The algorithms considered include AES, DES, 3DES, RC6, Blowfish, and RC2. The simulation results may be used to make several conclusions, including the fact that Blowfish outperforms all other approaches. Following that, RC6 is the best algorithm in terms of power and time consumption. The International Journal of Cryptography and Information Security is a peer-reviewed journal devoted to cryptography and information security research. RC2 is also the method with the lowest CPU demand of all the algorithms. Because of the time-consuming factor, it puts a lot of strain on the CPU.

III. METHODS

AES: AES (Advanced Encryption Standard) is a symmetric block encryption standard recommended by NIST (National Institute of Standards and Technology) for information security. Both encryption and decryption are done using the same key. It has a changeable key length of 128, 192, or 256 bits; the default is 128, 192, or 256 bits. It encrypts 128-bit data blocks in 10, 12, or 14 rounds, depending on the key size.

The most advanced and efficient encryption techniques for cloud storage are ECC and AES. Because of its higher key size, single AES is a little slower than the hybrid (ECC-AES) approach for data protection, whereas the hybrid technique has a smaller key size and a quicker security mechanism for data protection. Because the smallest key size is ECC's biggest advantage, AES reduces the key size and improves performance when it uses it for encryption. ECC uses encryption and decryption key standards to minimise key size and create a secure key system. To keep data protected against unauthorised access, ECC is the ideal approach to use in combination with AES. ciphertext will produce the data encryption after you've provided the key size and decryption. The key produced by ECC is used by AES. To get the secured system, the suggested approach at cloud storage is suited for the combined effect of both ECC and

AES. This helps to minimise storage size by using secure data.

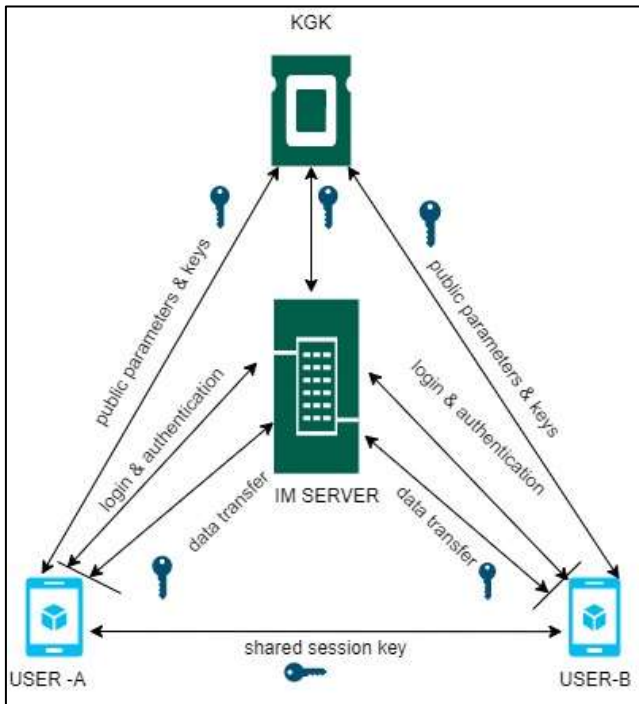


Fig. 1: Basic diagram of AES with ECC

A. Hashing Cryptography

Hashing is a cryptographic method for converting any type of data into a single string of text. Any piece of data, regardless of size or nature, can be hashed. The hash that any data produces with classical hashing is always the same length, regardless of the size, type, or length of the data. A hash is supposed to be a one-way function: you can put data into a hashing algorithm and obtain a unique string, but you can't understand the input data it represents if you come across a new hash. The hash of a unique piece of data will always be the same. A hash function is a function that calculates the sum of two numbers. H is a computationally efficient algorithm. takes as input an arbitrary-length message M and, in the case of a keyed hash function, a fixed-length key K, it produces a fixed-length output D termed the message digest. $D = H(K, M)$ D stands for Message Output, K is for Fixed Key Length, and M stands for Input Message Length. The following is a description of several commonly used terms. The following are some hashing cryptographic algorithms: MD5

B. MD5

(Message Digest5) is a frequently used 128-bit cryptographic hash technique. It transforms a variable-length message into a fixed-length output of 128 bits . The input message is divided into 512-bit chunks and padded to make the message length divisible by 512 bits. The sender encrypts the communication with the recipient's public key, and the recipient decrypts it with the recipient's private key.

C. RC6 is a fast block cypher (Rvest cypher 6):

It was based on RC5 and is quicker than RC5 since it has more registers. The RC6 algorithm employs integer multiplication. Unlike RC5, every word bit in RC6 is rotation dependent, whereas the non-essential bits in RC5 are not.

The following table, which is separated into five categories, compares AES, RC6, ECC, RSA, MD5, RSA, and DSA.

Scheme	Algorithm Type	Key Length	Rounds	Block Size
AES	Symmetric	128,192,256 bits	10,12,14	128 bits
RC6	Symmetric	40-128 bits	-	64 bits
ECC	Hashing	192 bit,256 bit	-	--
RSA	Asymmetric	1024 bit	1	Min. 512 bits
MD5	Hashing	128 bits	-	512 bits

Table 1: Different Security Algorithms method Config.

Algorithms, key lengths, rounds, and block size are all factors to consider. The key sizes of each algorithm varies from one another. A 128-bit key length is used in the MD5 algorithm. The key size for the AES algorithm is 128, 192, or 256 bits. The RC6 algorithm has a key size of 40-128 bits. The RSA algorithm employs a 1024-bit key size. The following parameters were used to test the performance of the supplied algorithms on a local system with varied input sizes in this experiment. This section describes the experimental settings, platforms, and essential management of experimental algorithms.

1) Evaluation parameters The performance of the encryption algorithm is evaluated using the following parameters

- 1) Encryption Time: The encryption time is the time it takes an encryption algorithm to convert a plain text into a cypher text.
- 2) Decryption Time: The decryption time is the time it takes a decryption algorithm to convert an encrypted text to plain text.

2) Platforms for Evaluation The following system configuration is used to test the encryption algorithm's performance.

- 1) Software Specification: Experimentation on Windows 10 Pro 32-bit version November 2017 Operating System. processor 1GHz
- 2) Hardware: All algorithms are run on an Intel Core i5 (2.40 GHz) seventh generation processor with 4GB of RAM and a 1 TB hard drive. Lenovo ideapad 520S

Key Management by the Algorithm Key management is the most important and core aspect of a cryptosystem for protect the data. If the key is strong and secure against unauthorised access, cryptography methods will be more effective. We use AES 256 bits keys, ECC 192-256 bits keys, MD5 512 bits keys, RC6 40-128 bits keys, and RSA 1024 bits keys in our experience.



Fig. 2: Encryption time of different algorithm (column based)

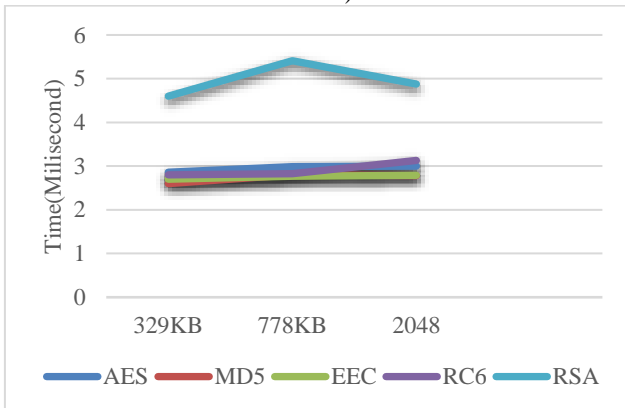


Fig. 3: Encryption time of different algorithm (line based)

Figures 2 and 4 show encryption and decryption timings for symmetric (AES, MD5, DES, and RC6) and asymmetric (AES, MD5, DES, and RC6) methods, respectively (RSA). As seen in the preceding pictures, symmetric encryption/decryption techniques are quicker than asymmetric encryption/decryption approaches in general. Furthermore, all algorithms in both categories (symmetric and asymmetric) have a proportionate connection between running time and input file size, with the exception of the DES and RSA algorithms. The AES and EEC execution times change somewhat as the size of the input file is greater. Table-2 is looked at. The RSA algorithm takes substantially longer to encrypt and decrypt than the AES, BLOWFISH, DES, and RC4 algorithms.

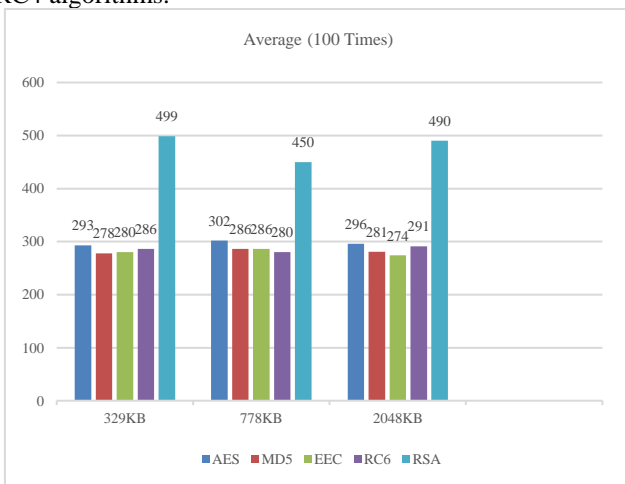


Fig. 4: Decryption time of different algorithm (column based)

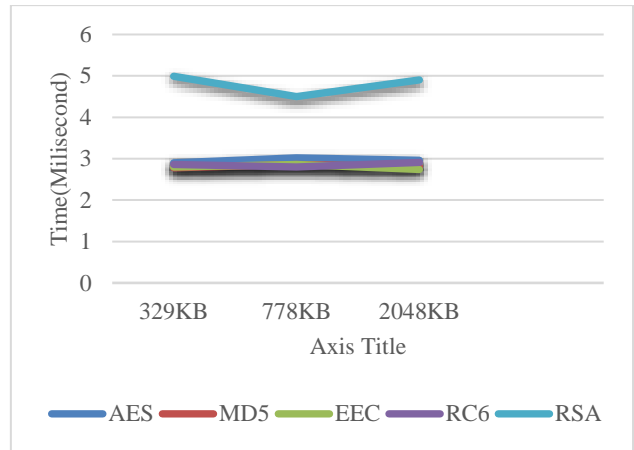


Fig. 5: Decryption time of different algorithm (line based)

IV. CONCLUSION AND FUTURE OBJECTIVES

Encryption and decryption methods are increasingly important for the security of communication through a cloud server in a wireless network. The data processing flow and temporal complexity of existing access control systems are investigated in this study. The performance of frequently used encryption algorithms such as AES, MD5, and RSA, as well as innovative techniques, is investigated in this study. The AES technique take the less time for encryption, whereas the RSA approach take the most, according to the text file utilized and the experiment outcomes. We are also show that AES decryption is superior to alternative algorithms based on the analytical results. We can say that the AES method is significantly superior to the RSA, MD5, and RC6 algorithms when considering picture, text, and audio data as input. Cryptographic algorithms such as AES, RSA, and MD5 will be compared and analysed in order to improve encryption and decryption speeds. We also discovered that the new algorithm is more theoretically sound.

REFERENCES

- [1] (Stallings, Network Security Essentials Applications and Standards, 2014), Fifth Edition
- [2] (Rizk & Alkady, Two-phase hybrid cryptography algorithm for wireless sensor networks, 2015), Journal of Electrical Systems and Information Technology, port said Egypt ;/www.sciencedirect.com
- [3] (Ahmed & Nader, 2016), "NEW ALGORITHM FOR WIRELESS NETWORK COMMUNICATION SECURITY" International Journal on Cryptography and Information Security (IJCIS), vol6, No. 3/4, December 2016
- [4] Dr. Sami S. Al-Wakeel and Eng. Saad A. AL-Swailem, "PRSA: A Path Redundancy Based Security Algorithm for Wireless Sensor Networks". This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.
- [5] Hendra Pasaribu, Delima Sitanggang, Rudolfo Rizki Damanik, Alex Chandra Rudianto Sitompul, "Combination of advanced encryption standard 256 bits with md5 to secure documents on android smartphone".

- IOP Conf. Series: Journal of Physics: Conf. Series 1007
(2018) 012014
- [6] Saba Rehman , Nida Talat Bajwa , Munam Ali Shah , Ahmad O. Aseeri and Adeel Anjum ; “Hybrid AES-ECC Model for the Security of Data over Cloud Storage”, <https://www.mdpi.com/journal/electronics>
- [7] Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Intia; “Performance Analysis of Different Cryptography Algorithms”, International Journal of Advanced Research in Computer Science and Software Engineering
- [8] Jianhua Peng, Hui Zhou, Qingjie Meng, Jingli Yang; “Big data security access control algorithm based on memory index acceleration in WSNs” ; EURASIP Journal on Wireless Communications and Networking.
- [9] Ronald L. Rivest. The MD6 Hash Function. To be released fall 2008.
- [10] <https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats>
- [11] <https://hackernoon.com/cryptographic-hashing-c25da23609c3>

