iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XII **Month of publication:** December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76199

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

Multi User Chat System using RSA Encryption and Signature with SHA-512 Hash

Balamurugan Aathavan
School of Information Technology and Engineering, VIT Vellore

Abstract: ***In this paper we have implemented a multi-client secure chat system based on client/server architecture. Every client will almost certainly talk to different clients all the while (many-to-many) and share information and among themselves. Throughout the years chat framework which is an application or apparatus utilized for imparting between at least two people over a system, has been faced with issues of security, information integrity and privacy of data/information. Since every client is viewed as a trusted client, other are plain text attack which makes communication vulnerable against spying, The motivation behind this exploration is to build up a verified chat framework condition utilizing RSA encryption and Digital Signature, the Digital Signature is utilized to build up a protected communication channel, giving an improved verified strategy for verification of the chat system.***

Keywords: chat, client, decryption, digital signature, encryption, hashing, server.

.

I. INTRODUCTION

In prior days, when communication needs to happen between 2 or three individuals communication happened just through phones or through letters. Yet, it is time taking method for speaking with individuals and furthermore costlier method for speaking with one another. Multi User Chat System is an application through which the client can speak with different clients associated in a same network area (LAN). To set up a communication between the frameworks, we need basic socket connections to interface them in a network. Socket programming utilizes the client attachment and server attachment techniques to interface the local host to the named host and port. The communication between different clients is finished utilizing client server model. A few client machines are associated with their server ports and communication is built up. To verify the communication between the client and server, RSA encryption is being used. It is an asymmetric (public key) crypto framework dependent on number hypothesis, which is a block cipher system. Its security depends on the trouble of the huge number prime factorization, which is a notable numerical issue that has no compelling solution. RSA public key cryptosystem is a standout amongst the most ordinary ways that most broadly use for public key cryptography in encryption and digital signature norms. The verified chat framework is intended to give security, confidentiality and integrity of communication between people involved by using the underlying technologies of RSA algorithm digital signature as its method of authentication and verification of users.

A. Approach

1) Creating the basic chat server
2) Handling the user presence
3) Sending Direct messages
4) Creating the chat client API
5) Building the client GUI
6) Adding encryption and decryption functions
7) Deriving integrity by hashing
8) Authentication by Digital Signature

TCP/IP: Short for Transmission Control Protocol/Internet Protocol, TCP/IP is a set of rules (protocols) governing communications among all computers on the Internet. TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. The TCP part has to do with the verifying delivery of the packets. The IP part refers to the moving of data packets between nodes. TCP/IP can be used as a communications protocol in a private network

RSA: Rivest– Shamir– Adleman is one of the first public key cryptosystems that was utilized for information transmission. Two large prime numbers are picked and used to create the public and private keys through a algorithm.
RSA takes a shot at the infeasibility of considering that item. With adequately sufficiently vast primes, the factorization turns out to be excessively computationally burdening and almost incomprehensible. When the Private and Public keys are produced, the public key is sent to the gathering who will send the message. That party will encode their plaintext into ciphertext utilizing that public key and send it (plaintext) back to the person who produced the keys in any case. The recipient will at that point utilize his secret private key to decrypt the ciphertext back to plaintext and see the actual message.
Socket*:* Socket Programming is a method for associating two hubs on a system to speak with one another. One socket(node) tunes in on a specific port at an IP, while other attachment contacts the other to frame a connection. Server frames the listener socket while client connects with the server. Socket Programming is begun by bringing in the socket library and making a straightforward attachment.

II. LITERATURE SURVEY

1) In this paper the author proposed communication be-tween different processes through the serial ports available in the computer. The proposed implementation in this paper was using UNIX socket programming using C++ programming language. The proposed concept of sockets was inferred.

2) The concept of server client communication was introduced in this paper. Communication through socket of the computer is being proposed. TCP protocol has been adapted for exceedingly productive communication

3) In this paper the author proposed the concept of digital signature using three algorithms for testing the authentication of the data. The proposed RSA algorithm was implemented in this paper for testing the authentication of the message sent to the server by each client and the message sent by the server to each client.

4) In this paper the author proposed an approach to keep up the integrity of the information, a system is made which is known as a digital signature. A digital signature is a particular code which is created from the capacity of delivering a digital signature. One of the calculations that are utilized to make the digital signature is a hash work. There are many hash functions. Two of them are Message digest 5 (MD5) and SHA256. These the two calculations absolutely have the benefits and weaknesses of each. The reason for this exploration was to decide the calculation which is better. The parameters used to look at that two calculations are the running time and complexity. The examination results got from the complexity of the calculations MD5 and SHA256 is the equivalent, i.e., Θ (N), yet with respect to the speed is gotten that MD5 is better contrasted with SHA256.

5) This paper talked about the security of SHA-256, SHA384 and SHA-512 against the collision attacks and gave some understanding into the security properties of the essential structure. It was presumed that neither Chabaud and Joux's assault, nor Dobbertin-style assaults applied. Differential and linear attacks likewise didn't matter on the fundamental structure. Anyway, the author demonstrated that the slightly streamlined forms of the hash functions are shockingly weak: at whatever point symmetric constants also, initialization values were utilized all through the calculation. In this manner, the complex nature of attack on these altered hashes worked and possibly progressed toward becoming as low as one wish.

6) The author of this paper proposed the most well-known digital signature calculations such as DSA, RSA and ECDSA and thought about these calculations. These signature calculations were executed with different unique key sizes set. Trial examination aftereffects of the three signature calculations were exhibited and investigated by the author. The outcomes demonstrated that ECDSA was increasingly reasonable to create the mark and RSA was increasingly reasonable to confirm the verification. The aftereffects of this paper were displayed to demonstrate the adequacy of every calculation and to pick the most appropriate calculation for Digital signature.

7) The author of this paper proposed the key element of public key cryptosystem in which the encryption and decryption system are finished with two diverse keys - public key and private key, and the private key cannot be gotten from the public key, that empowered the distribution of the encryption key without the danger of releasing the secrets The most huge methodology of public key cryptography calculation is RSA, which opposed practically all the known passwords attacks up until this point.

S.no	Title	Methods and Techniques	Advantages and disad-vantages
1.	Socket programming in the data communications laboratory [1]	Peer to peer chat program, multiple chat program, use of socket communication	Advantages Possibility of inter-process communication using the sockets Disadvantages Method followed here is very old
2.	The socket programming and software design for communication based on client/server [2]	Client server architecture	Advantage It makes many clients share the same access to sources of information. Disadvantage Too many requests from the clients may lead to congestion, which rarely takes place in P2P network.
3.	Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5) [3]	RSA encryption technique for data integrity.	Advantages The digital signature attached by the sender to the document can be used as a tool to ensure that the submitted document is authentic or not manipulated. Little change of the file can affect the validation result. Disadvantages Results in large computational overheads and slows down the system considerably.
4.	Research and implementation of RSA algorithm for encryption and decryption [4]	Encryption, decryption using RSA	Advantages Provides stronger identity checking through secret private keys. Disadvantages Not very scalable: Distribution of public keys can be cumbersome in large environments
5.	Secure encryption with digital signature approach for Short Message Service [5]	Signature for the messages sent by the client to the server and the server to all the clients	Advantage Authentication of the message can be verified Disadvantage Computational overhead
6.	Analysis of SHA-512/224 and SHA-512/256 [6]	Performance comparison between hashing algorithms.	
7.	A comparative study of Message Digest 5(MD5) and SHA256 Algorithm [7]	The two algorithms are compared based on 2 parameters which are the running time and the complexity	Advantages MD5 collisions have been contrived 'in the laboratory' Disadvantages The research results obtained from the complexity of the Algorithms MD5 and SHA256 is the same, i.e., Θ (N), but regarding the speed is obtained that MD5 is better compared to SHA256
8.	Security Analysis of SHA-256 and sisters [8]	studies the security of SHA-256, SHA-384 and SHA-512 against collision attacks and provides some insight into the security properties of the basic building blocks of the structure	Advantages SHA 256 is a one-way func-tion that is deterministic, fast to compute, resistant to preimage and second-preimage attacks, and is collision resistant. Disadvantages It's shown that slightly simplified versions of the hash functions are surprisingly weak

Table 1: Techniques and Drawbacks

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

III. IMPLEMENTATION OF RSA

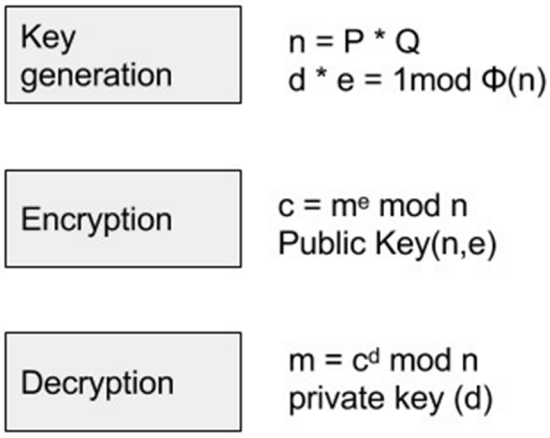


Figure1: Overview of RSA

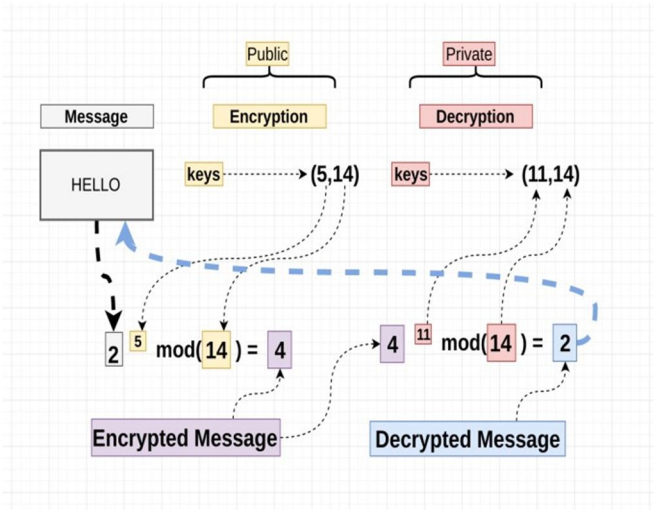


Figure2: Working of RSA

To actualize RSA cryptosystem, which is a troublesome procedure, which involves the generation of prime numbers, large arithmetic and other mathematical calculations are to be performed. In RSA cryptosystem, p and q are very large prime numbers. To accomplish it, the most essential factor is the efficiency in generate large prime numbers.

First, the generation procedure of keys is as follows,

1) Randomly generates two large primes P and Q of length K / 2 bit;
2) Calculate the public key: publicKey=P*Q; (public Key's length is k-bit)
3) Generate a random encryption key: keyE, 2<=keyE<=<D(n)-I, where GCD (keyE, <D(n)) =I;
4) This is the necessary conditions for the finding of the decryption key keyE * keyD mod <D(n)=I, <D(n) is known as the Euler function of n, the value is <D(n)= (P- 1) *(Q-l)
5) Calculate the decryption key: keyD=keyE-l mod (n), keyE-l is inverse for the decryption key keyD. The formula of the original equation is keyE * keyD mod <D(n)=1
6) The public key, encryption key and decryption key are all calculated.
7) Then, the process of encryption of the plaintext and decryption is done
8) Encryption: C = MkeyE mod publicKey; M denotes the plaintext, and C denotes the ciphertext.
9) Decryption: M = CkeyD mod publicKey; in which M denotes the plaintext, C denotes the ciphertext.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

IV. MATHEMATICAL MODEL FOR THE DIGITAL SIGN TURE AUTHENTICATION OF THE SYSTEM

The clients on enrolment are made to create a record which is put away in an exhibit connected rundown hash table database situated at the server end of the framework; the enrollment is finished when a client gives a username and produces the private key modulus and type created from condition 1, 2, 3

$c = (M^e \, M \, o \, d \, N)$ ---------- (1)

$512 < e < \emptyset(N)$ ----------(2)

Where p is the set $512 \leq p \leq 1024$ and

$512 \leq q \leq p$, $\emptyset(N) = (p-1)(q-1)$ ---------- (3) The modulus and exponent are used to perform the signature operation as shown in equation 4 at the request for private communication by a client

$N = p \times q$ ---------- (4)

The receiver should likewise set up a private association by producing his private and public keys separately. The message sent by the client is encoded utilizing the senders private key and is just decoded utilizing the senders public key, along these lines for the first message to reach the recipient, the receiver and the sender must have established a two-way handshake protocol of their respective public keys and the check of the procedure is given by the condition 5

$M = C^{d}{}_{m \, o \, d \, N}$ ---------- (5)

The keys generated are computer generated in 512 bits binary form and must be copied for signature/verification purposes

V. PROPOSED ARCHITECTURAL MODEL

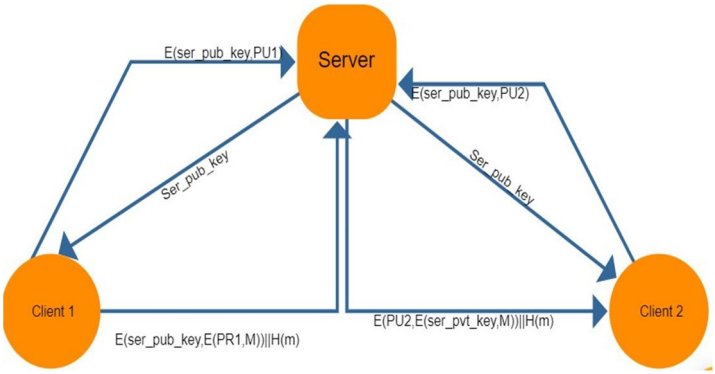


Figure 3: Key exchange and message exchange

1) Ser_pub_key: Public key of server
2) Ser_pvt_key: Private key of server
3) PU1: Public key of client 1
4) PR1: Private key of client 1
5) PU2: Public key of client 2
6) PR2: Private key of client 2

Figure 4: Model for sending message

7) PUa: Public key of A
8) PRa: Private key of A
9) PUb: Public key of B
10) PRb: Private key of client B

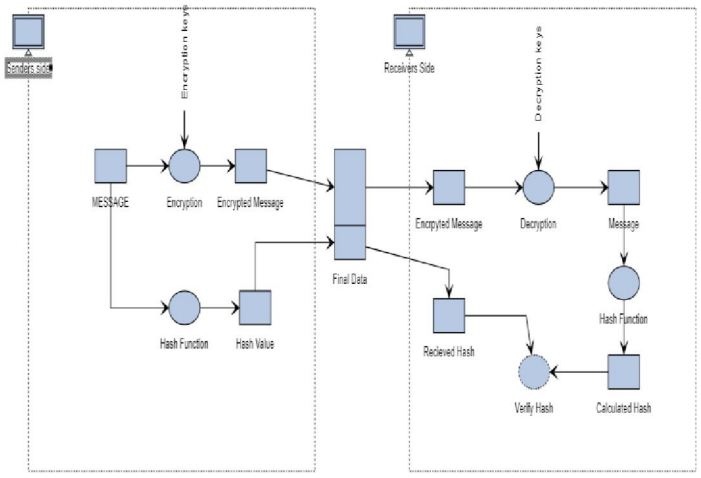


Figure 5: Model for data validation

VI. IMPLEMENTATION OF CHAT SYSTEM

Figure 6: The server displaying the clients connected. Once the message is received the server encrypts and send the message to every client.

Figure7: Key exchange between client and server. Similarly, key is exchanged for any new clients

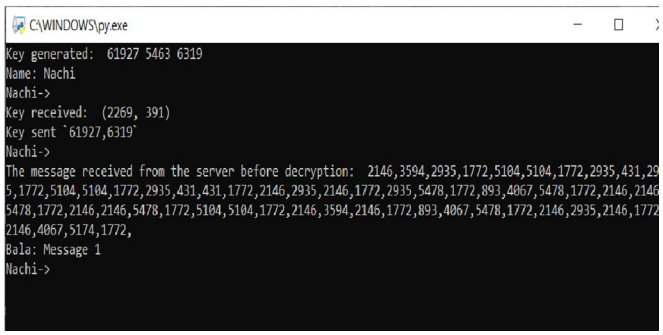


Figure 8

Figure 9: Encrypted message with the hash and signature sent to the client and message is displayed after decryption.

VII. METRICS

Algorithm used	Message used for comparision	Average time for encryption (ms)	Average time for decryption (ms)
DES	encryption encryption encryption	16.987800	13.927459
AES	encryption encryption encryption	162.530899	0.0
ELGAMAL	encryption encryption encryption	4.2543411	3.7243366
RSA (Implemented in this paper)	encryption encryption encryption	4534.7514	3912.322521

Table 2: In this comparison it was found that the RSA algorithm used here takes longer time to encrypt and decrypt than other cryptographic algorithms. The time taken by the RSA algorithm solely depends on the size of the key it uses.

VIII. CONCLUSION

In this research a secure multi user chat system was achieved using the RSA algorithm for encryption and decryption of the message using the server's public key and private key and the client's public key and private key, the authenticity of the message was verified using an RSA based signature. To test the integrity of the message SHA-512 hashing algorithm was implemented. This system implements a very secure systems, thus the computational overhead of the system is high.

REFERENCES

[1] Toll, W. E. (1995, March). Socket programming in the data communications laboratory. In *ACM SIGCSE Bulletin* (Vol. 27, No. 1, pp. 39-43). ACM.

[2] Xue, M., & Zhu, C. (2009, May). The socket programming and software design for communication based on client/server. In *2009 Pacific-Asia Conference on Circuits, Communications and Systems* (pp. 775-777). IEEE.

[3] Ardy, R. D., Indriani, O. R., Sari, C. A., Rachmawanto, E. H. (2017, November). Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5). In 2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS) (pp. 87-92). IEEE.

[4] Zhou, X., & Tang, X. (2011, August). Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of 2011 6th International Forum on Strategic Technology (Vol. 2, pp. 1118-1121). IEEE.

[5] Saxena, N., & Chaudhari, N. S. (2012, October). Secure encryption with digital signature approach for Short Message Service. In 2012 World Congress on Information and Communication Technologies (pp. 803-806). IEEE.

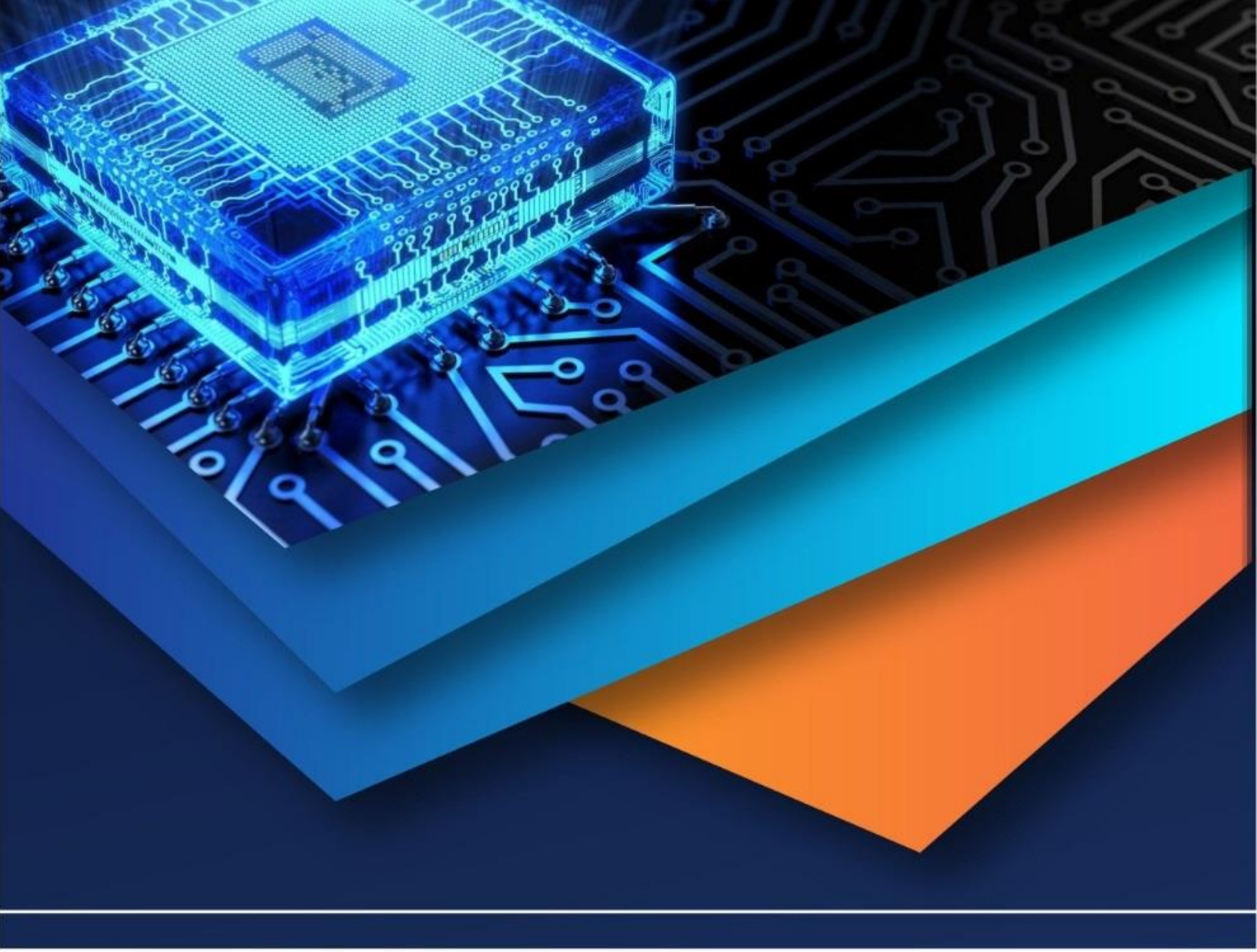
[6] Dobraunig, C., Eichlseder, M., & Mendel, F. (2015, November). Analysis of SHA-512/224 and SHA-512/256. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 612-630). Springer, Berlin, Heidelberg.

[7] Rachmawati, D., Tarigan, J. T., & Ginting, A. B. C. (2018, March). A comparative study of Message Digest 5 (MD5) and SHA256 algorithm. In Journal of Physics: Conference Series (Vol. 978, No. 1, p. 012116). IOP Publishing.

[8] H Gilbert, H Handschuh Gilbert, H., & Handschuh, H. (2003, August). Security analysis of SHA-256 and sisters. In International workshop on selected areas in cryptography (pp. 175-193). Springer, Berlin, Heidelberg.

[9] https://www.yworks.com/products/yed-live online tool for diagrams

[10] https://samsclass.info/141/proj/pCH-RKF.htm
[11] Stallings, W. (2017). Cryptography and network security: principles and practice (pp. 92-95). Upper Saddle River: Pearson.
[12] https://stackoverflow.com/
[13] https://pypi.org/
[14] Huston, G., & Michaelson, G. (2016). The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (No. RFC 7935).
[15] Danasingh, Asir Antony. (2016). Performance Analysis of Data Encryption Algorithms for Secure Data Transmission. International Journal for Science and Advance Research in Technology. 2. 388-390.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY