iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44050

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 10 Issue VI June 2022- Available at www.ijraset.com

Distributed Computing of DNA Cryptography and Randomly Generated Mealy Machine

Sushma N K[1], Dr. Ravikumar G K[2], Ms. Sindhu D[3]
[1]*Dept. of CSE, BGS Institute of TechnologyAdichunchanagiri University, BG Nagar, Karnataka,India-571448.*
[2]*Professor & Head(R&D)Dept. of CSE, BGS Institute of Technology, Adichunchanagiri University, BG Nagar, Karnataka, India-571448*
[3]*Dept. of ISE, BGS Institute of Technology, Adichunchanagiri University, BG Nagar, Karnataka, India-571448*

Abstract: ***The volumes of information created and saved in operating systems are growing at an alarming rate these days. Between all of these devices, massive volumes of essential and sensitive files are transmitted. As a result, ensuring the protection of all of these irreplaceable data is critical. Cryptography is a well-known method for ensuring data security. Cryptography's main goal is to transmitthe information from the source to the destination in the most secure method possible, preventing an adversary from extracting the actual datainformation. This research suggests a novel cryptographic algorithm depending on DNA encryption and the notion of restricted automata. The system consists of three components: cryptographic keys, a generator, a transmitter, and a transceiver. Based on the features of the receiver, the transmitter generates a 256-bit DNA-based secret key, which is used to encrypt information. The DNA sequence is then coded using a procedurally generated Mealy machine, that provides the ciphertext more safe. The suggested approach can defend the system from a variety of security attacks. This technique has proven its capacity to provide an individual user with better safe storage by dividing the user's vital information into bits.***

Keywords: Cryptography, DNA, Ciphertext, Data.

I. INTRODUCTION

Cryptography is widely regarded as the most effective method of protecting data protection. The main purpose of cryptographic is to transfer data from the transmitter to the recipient in a disguised form across an insecure communication medium, making it impossible for an attacker to get access to the original source. Cryptography is divided into twotypes: symmetric cryptographic encryption and asymmetric cryptographic encryption, strictly speaking. In symmetric-key encryption, the keys are symmetric, the encryption and decryption procedures utilize the same key (Kumar and Wollinger, 2006; Schneier, 1996), whereas in asymmetric key encryption, the encryption and decryption operations use two separate keys. The private and public keys are the two types of keys. The key must be kept private, while the public key is shared with everyone.

The field of DNA encryption is a relatively new one that has evolved as a result of the advancement of DNAcomputing (Sundaram et al., 2015). Unlike traditional encryption, DNA cryptography ensures data security by combining DNA features with cryptographic techniques. The data protection has become a serious worry due to rapid advancements in the context of computer innovation and the daily processing of massive amounts of data. DNA cryptography is now frequently employed in the encryption area. Severaltechniques based on DNA cryptography have been developed by many researchers to increase data storageand data security. All of these schemes have been discovered to have security flaws. Furthermore, some schemes take an unreasonable amount of time to generate and retrieve secret keys.

II. RELATED WORK

Different cryptographic algorithms for transmitting data efficiency and security have been developed and been implemented by many researchers in the last few years. In this part, we look at some of the implementations. Gsm Models were used to explore the Data Encryption Standard (DES) algorithm Rama et al. (2012). (CA). The capacity to generate numeric keys throughout data access is required in this method, and the DES algorithm can be easily implemented using cellular automata rules. For key generation, CA rule number 30 is applied. The key size is just 48 bits, despite the fact that this constraint is for processing randomness. Sharma et al. (2013) suggested a text transfer approach that is both secure and reliable. The goal of this method is to give two degrees of protection. A passcode is used to mask the text in thefirst phase, and 2-D cellular restrictions are utilized to secure the data in the second level.

©IJRASET: All Rights are Reserved

If the first degree of security is breached, the second degree of security ensures that the transmitted message is kept safe. Encryption is done using two- dimensional cellular automata rules. The significant key generation time is a drawback of this technology. Sony et al. (2013) suggested a new DNA cryptography technique is on the basis of Moore machine concept from automata theory.

This technique's security is based on three encryption stages: a secret key, an auto-generated Moore machine, and a password. The message is initially encrypted using just a private key which is dynamically created in Sony et al technique. .'s The cipher text is converted into binary sequence that is divided into 'n' blocks of 256 bits each. The blocks are subjected to the Exclusive OR (EXOR) operation, with the results being translated into a Genetic code using a code generator (lookup table). The user's passcode is generated by feeding the DNA sequence into a Moore machine. Using a codebook, the freshly constructed passcode is turned into a DNA sequence once more. The ultimate encrypted data supplied to the receiver is this DNA sequence. This approach, however, is quite sluggish.

Hossain et al. (2016) suggested latest DNA cryptography method that use a DNA sequence database to improve security. Initially, a DNA sequence database is assigned with ASCII characters. A fixed number of parameters are conducted to a numerical series throughout each data transmission method changing the location of the ASCII letters in the sequence table dynamically. The updated binary value is then subjected to a OTP. The OTP encrypted message is once again processed using genomic conversion. Finally, an amino acid database containing protein sequences is used to compress the ciphertext, increasing the ciphertext's confusion.

Kalyani and Gulati (2016) suggested a three-level security technique for safe data transmission, namelya metabolic mechanism, an arithmetic operation, and an OTP system. First, the data is transformed to a binary sequence. After then, the digital sequence is EXORed with an OTP. The binary sequence obtained is translated to a DNA sequence using the following rules: 00=A, 01=T, 10=C, and 11=G. The basic rule is then used to create a new Sequence of dna. To retrieve the final encrypted information, the sequence is reversed and supplied to the receiver.

III. RESEARCH METHODOLOGY

To achieve reliability and economies of scale, cloud services, like a utility delivered over a system, relies on resource sharing. The bigger concept of interconnected infrastructure and shared services underpins cloud computing. Cloud services has numerous advantages, but it also comes with a slewof security concerns and threats. Due to the hazards of service disruptions, using simply a "single cloud" server seems to be less popular, data theft, and data leaking, as well as the likelihood of a dangerous insider attack. The usage of many clouds, often known as "multi-clouds," "inter-clouds," or "cloud- of-clouds," is a materialized solution to this problem. Users' vital data will be split into pieces and various intriguing aspects of biological DNA sequences as well as information hiding principles will be used to it in order to improve data availability and security. Finally, the DNA encoded data bits will be distributed throughout the Cloud Service Providers that are available (CSP). As a result, our research suggests a feasible answer to cloud security and privacy concerns.

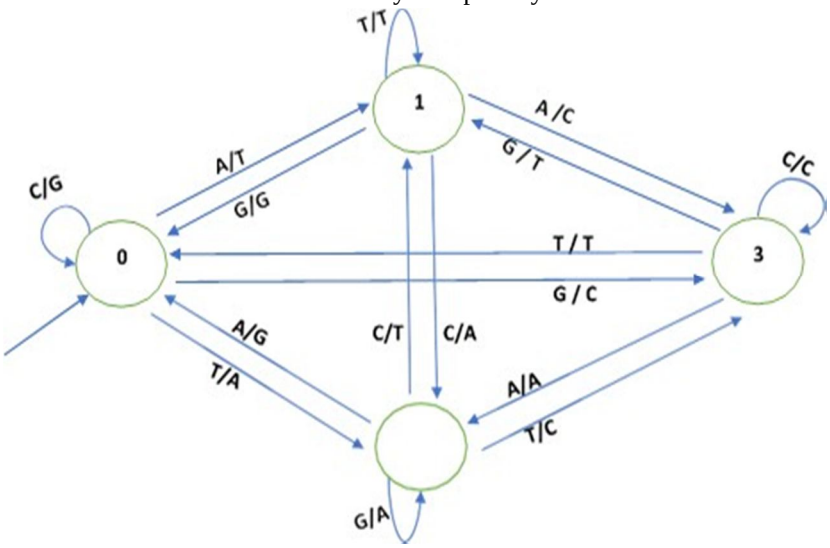


Fig1. Design of the Mealy machine.

The purpose of the proposed strategy is to constructa protect its data transfer system from one sender to another. There will be three entities in following system are:

1) Key-Pair Generator (KPG): This entity gives cryptographic keys to the transmitter and transceiver throughout the procedure for registering

2) Transmitter: These object keeps both sensitive and non-sensitive information.

3) Transceiver: This object is accepted or rejected to the transmitter for any required data to be received.

On request, the KPG initially sends the pivotal to the transmitter and transceiver. The keys are used to exchange the confidential parameters that are requested for keys to encrypt and decrypt data. The transceiver sends an access request to the transmitter, along with some information about the recipient. The transmitter uses the KPG to verify the transceiver identity. If the transceiver has been verified, the transmitter will generate a 256-bit Transceiver Attributes Secret Key (TASK). The encryption key is turned into a Sequence of dna once it has been encrypted with RASK. The DNA sequence is fed into a Mealy machine that generates the cipher text after randomly transforming the input into latest DNAsequence. The suggested system is made up of a small number of components. (i) system configuration (ii) Transceiver registration (iii) key creation (iv) DNA-based Mealy machine generation (v) data encrypting, and (vi) data decoding The full system's workflow is depicted in Figure 2.

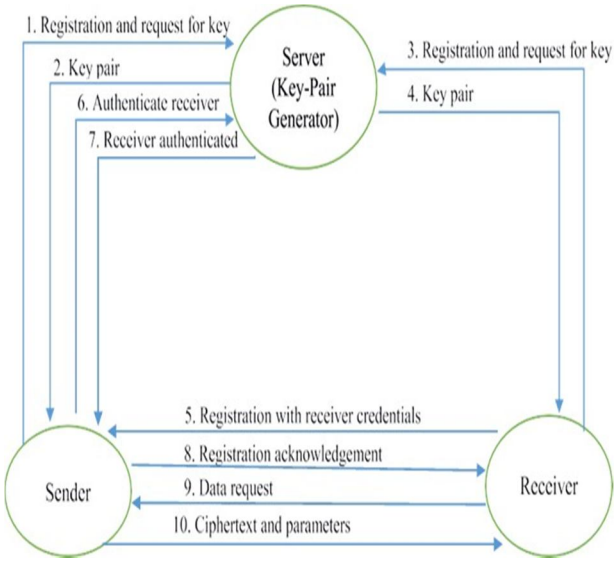


Fig2. The suggested scheme's work flow.

A. Initialization of the System

A registration request is sent to the KPG by boththe transmitter and the transceiver. For the transmitter and transceiver, the KPG produces private key pairs. The entities are issued key pairs, with the secret key kept hidden by the another entities.

B. Transceiver Registration

The transceiver sends the sender a registration request that includes some of the receiver's personal information, such as the PAN, email, MAC address. The properties are encrypted and sent using the recipient's secret key and also the user's public key. From the KPG, the sender certifies the receiver's authenticity. An acknowledgment is delivered to the receiver if the authentication is successful.

C. Key Generation

The transmitter starts the key creation method with different attributes obtained from the receiver. The parameters provided in encoded format aredecoded using the user's secret key and the recipient's session key. Table is used to translate the values into their ASCII equivalents. As a result, the generated ASCII characters are substituted with their binary data. If the final default value is less than 256 bits, extra zeros are added to the end of the binary integer. If this is not done, extra bits are clipped from either the beginning of the end of the binary values. As a result, a 256-bit cryptographic keys (TASK) is produced.

D. Data encryption

The transmitter chooses the content as well as converting every specific character ASCII value. The binary string is then formed by converting every ASCII character to its binary data. If the binary string's length (len) exceeds 256 bits, the digital phrase is partitioned upto 256-bit codeblocks. Then, amongst every 256-bit blocks or the 256-bit TASK, an EXOR operation is done. If the final unitis smaller than 256 bits, the RASK is truncated and The EXOR operator is applied to the final block.

Algorithm 1 – Encryption Algorithm.

Input: Plaintext
Output: Ciphertext

1. START
2. CONVERT each character of plaintext to ASCII values
3. CONVERT ASCII values to their equivalent binary string
4. IF len ≥ 256 bits
5. DIVIDE binary string into 256-bit blocks
6. EXECUTE EXOR between each 256-bit block and 256-bit RASK
7. IF len < 256 bits
8. EXECUTE EXOR between truncated RASK and binary string
9. SELECT R2 from Table 4
10. PERFORM DNA coding on the binary string to generate dnaD1
11. FOR each DNA base in dnaD1
12. APPLY transition rule to find the next state and the new DNA base
13. APPEND new DNA base to dnaD2
14. end FOR
15. REVERSE dnaD2
16. END

E. Data Decryption

To retrieve the ciphertext, the transceiver decodes the message using the recipient's secret key and the cardholder's session key, DNAMM, variables R1 and R2. The transceiver inverts the ciphertext before constructing the DNA sequence, dnaD2. Then, in reverse order, the methods of Section 3.4 are used to decode DNAMM. The Mealy machine's condition database and output table are so refreshed. Using his or her qualities, the transceiver has also recovered the 256-bit private key (TASK).

Algorithm 2 – Decryption Algorithm.

Input: Ciphertext
Output: Plaintext

1. START
2. REVERSE the ciphertext
3. DECODE DNAMM
4. FOR each DNA base in dnaD2
5. APPLY Tables 1 and 2 to find the next state and the new DNA base
6. APPEND new DNA base to dnaD1
7. end FOR
8. CONVERT dnaD1 to binary string
9. IF len ≥ 256 bits
10. DIVIDE binary string into 256-bit blocks
11. EXECUTE EXOR between each 256-bit block and 256-bit RASK
12. IF len < 256 bits
13. EXECUTE EXOR between truncated RASK and binary block
14. CONVERT binary string to equivalent ASCII values
15. CONVERT ASCII values to plaintext
16. END

IV. PROPOSED APPROACH

The suggested system's performance is measured using a Java platform implemented and 256 GB SSD, as well as Linux as the operating system. The key-pair generator is implemented using the Apache2web server. The transmitter and transceiver components are written in Java, and they communicate with the server via JSP. The data utilized to evaluate the suggested system comes fromthe 20 Message board data , which is a well-known dataset that has been used in numerous studies. This dataset was chosen because it provides textual data that may be used to test the suggested approach.

Six pieces of information from the dataset are used to evaluate the encryption and decrypt the data times, each of which is categorized according to its size. The time it takes to encrypt and decrypt data is calculated by running 50 trials for each input classification. Subsequently, the average values from the results were taken into account, as shown in Table 6. The present and proposed techniques' encrypting and decrypting timings are analyzed, and It has been discovered that perhaps the proposed system outperforms the competition in terms of encrypting and decrypting speeds, even when employing varied data amounts. The outcomes are depicted in the graphs. The encrypting time in the suggested system is lowered by 24%, while the decoding rate is reduced by 80%.

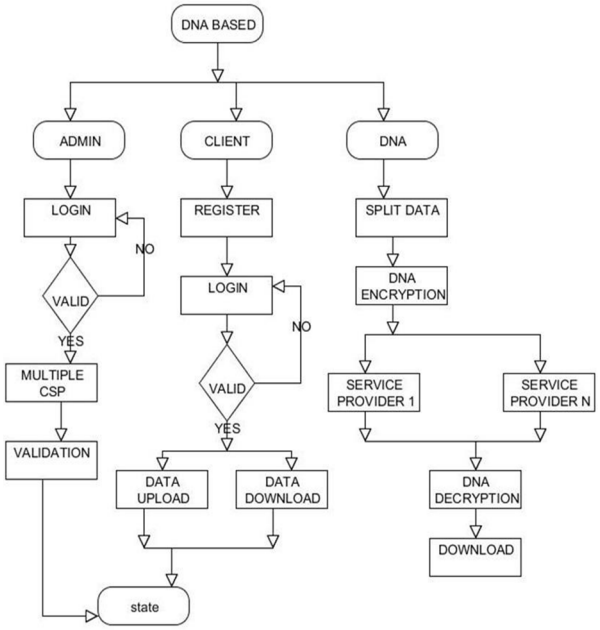


Fig3. Flowchart

The relationship between the data server and the client is the input style. It comprises defining model development requirements as well as standards, and also the steps necessary to transform metadata into processable data. This can be accomplished by examining a web page to check if it can accept data from a typewritten input, or by allowing users manually enter the data into the network. The goals of input design include restricting the number of actions required, controlling errors, eliminating delays, avoiding unnecessary phases, and simplifying the procedure. The input has been planned to provide safety and convenience while also retaining privacy.

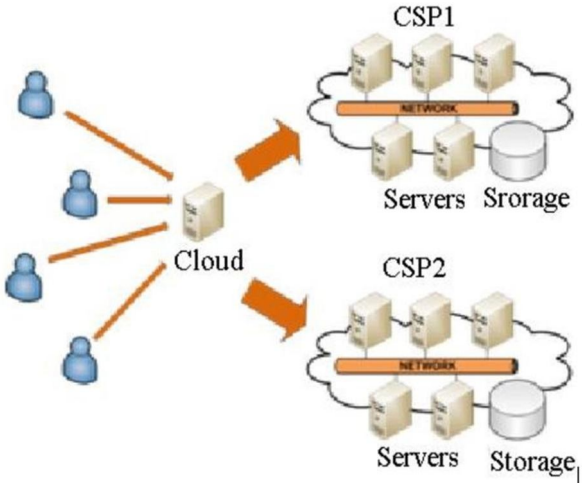


Fig4. System architecture

The process of transforming client feedbackneeds into a computer-based response is known as input design. This architecture is critical for eliminating redundant data and guiding management to the computerized system's dependable statistics. It is carried out by developing subscriber transaction management panels capable of handling large volumes of data. The inputting strategy's intention is to make information more effective and error-free. The data entry window is set up to allow you to perform all of the information manipulations.

It also helps to look at your files. Once the data has been entered, it will be validated. Information can be entered on screens. As needed, appropriate messages are given to ensure that the client has never been caught off guard. A performance management solution is one that satisfies the end-needs user's and properly shows data. The mechanism by which the outcomes of a program's processing are communicated to users and other organizations is known as outputs. How often the data will be transported for immediate usage, and also the hard copy output is determined by the output design. This is the most valuable and crucial source of information for the user, this is the most valuable and vital source of information. Through robust and sustainable output design, the service's relationship with the customer is improved.

The appropriate output should always be produced while also assuring that each outcome component is structured in a way that makes the system simple to use. When analyzing result of data, they should determine whichoutput is required to meet the criteria. Choose from a range of data presentation methods. Generate a paper, or document, that contains the informationfrom the system. The output form of an information system may meet one of its following goals. Provide information on historical activities, present events, orfuture estimates. Important events, opportunities, problems, or cautions should be announced. A response is elicited, and the response is confirmed.

V. RESULTS

Surveillance is used to look for errors. The process of seeking to uncover all conceivable defects or vulnerabilities in a bit of creative work is referred to as testing. Different components, sub-assemblies, composites, and/or the entire product can all be tested. It's the process of examining code to ensure that it adheres to specifications and satisfies the requirements of the users, and therefore that it just doesn't fail in unforeseen ways. Tests are available in a range of sizes and colors. Each test is tailored to a particular testing requirement.

Unit testing is the process of system testing to confirm that perhaps the project's basic functionality is operating correctly and that coding inputs create legitimate outputs. Every selected branching and produced code flow should undergo validation. It's a technique for putting the application's various software components through their paces. It's only done once each component is finished but before they're put together. This is a geometrical test that necessitates structural knowledge. Component methods are used to test an individual business process, software, or system configuration at the component level. Each process management path is tested to ensure that it follows the published criteria and has explicitly indicated inputs and outputs. According to economic and technological objectives, system requirements, and user manuals, functionality testing shows that the capabilities being tested are available.

Functional testing focuses on the following items: Valid Input: The types of valid input that have beenaccepted must be identified.

Invalid Input: Invalid input classifications must bediscovered and rejected.

Functions: It is necessary to use the capabilities thathave been discovered.

Output: The application outcomes that have beendiscovered should be put into the test.

It is necessary to use interfacing systems and procedures. Operational assessments are organized andproduced in accordance with requirements, functional areas, or distinctive test cases.

Furthermore, testing should include a thorough examination of organizational process flows, data fields, defined procedures, and following processes. Before operational testing is done, more tests are identified, and the efficiency-driven is established. The sequential testing of two or many software package modules on a shared framework Software integration testing is performed to simulate failures caused by interface deficiencies. The integration test assures certain modules or operating systems, such as those present ina technology platform or – as a significant upgrade – business-level software applications, perform seamlessly together. All of the above-mentioned test cases were successful. There were no defects to be found. Public Approval Testing is a crucial component of any project that necessitates the end user's active engagement. It also ensures that the system is compliant with the functional requirements. All of the test cases listed above were completed successfully. It was discovered that there were no flaws..

Table 3.Test cases status

Test case ID	Test case name	Test case description	Test steps				Test status P/F
			Step	I/p given	Expected o/p	Actual o/p	
TC01	Login	To verify that the User has entered Valid username and password	Login with Username &pswd	Valid Usn&Pswd	Login successful	Login successful	Pass
	Login	To verify that the User has entered Valid username and password	Login with Username &pswd	Invalid Usn& Pswd	Login successful	Error Enter valid Usn&pswd	Fail
TC02	Registration	To verify that the user has registered by entering valid details	Enter all the valid user details	Valid details	Registered successfully	Registered Successfully	Pass
	Registration	To verify that the user has registered by entering valid details	Enter all the valid user details	InValid details	Registered successfully	Not Registered Successfully	Fail
TC03	CSP	Uploads the data to the DNA,DNA will encrypt the data and send it to the CSP	Encryption of data	Encrypt Data	Decrypt the data and send it client	Decrypt the data and send it client	Pass
	CSP	Uploads the data to the DNA,DNA will encrypt the data and send it to the CSP	Encryption of data	Encrypt Data	Decrypt the data and send it client	Decrypt the data and send it client	Pass

VI. CONCLUSION AND FUTURE WORK

Businesses seeking a competitive advantage in today's market can profit from cloud computing, but security issues and risks are deterring adoption. By splitting the user's critical information into pieces, this strategy has proved its ability to include an internet user with better secure storage, advanced DNA-based encryption is applied to every component of the data before it is uploaded to several clouds. The applied concepts, on the other hand, are unquestionably helpful in constructing a solid cloud security infrastructure. This will surely meet client requirements, resulting in increased investment in both industrial and future research farms. The implementation of a malware scanner and malware detector, as well as their embedding into an application, is in the future scope of this study. This will prevent harmful material from being uploaded. Upload multimedia content data to the cloud using DNA-based encryption.

REFERENCES

[1] Baykara M, Gürel ZZ. Detection of phishingattacks. In: 6th International Symposium on Digital Forensic and Security (ISDFS); 2018. p. 1–5. doi:10.1109/ISDFS.2018.8355389..

[2] Chang X, Yan A, Zhang H. Ciphertext-only attack on optical scanning cryptography. Opt. Lasers Eng. 2020;126. doi:10.1016/j.optlaseng.2019.105901

[3] Clelland CT, Risca V, Bancroft C. Hiding messages in DNA microdots. Nature 1999;399(6736):533–4.

[4] Devi D, Namasudra S, Kadry S. A boosting-aided adaptive cluster-based undersampling approach for treatment of class imbalance problem. Int. J. Data Warehous. Min. (IJDWM) 2020;16(3):60–86.

[5] Gehani A, LaBean T, Reif J. DNA-based cryptography. In: Jonoska N, Paun G, Ozenberg G, editors. In: Aspects of Molecular Computing. Springer; 2000. p. 167–88.

[6] Gupta R, Singh RK. An improved substitution method for data encryption using DNA sequence and CDMB. In: Proceedings of the 3rd International Symposium; 2015. p. 197–206.

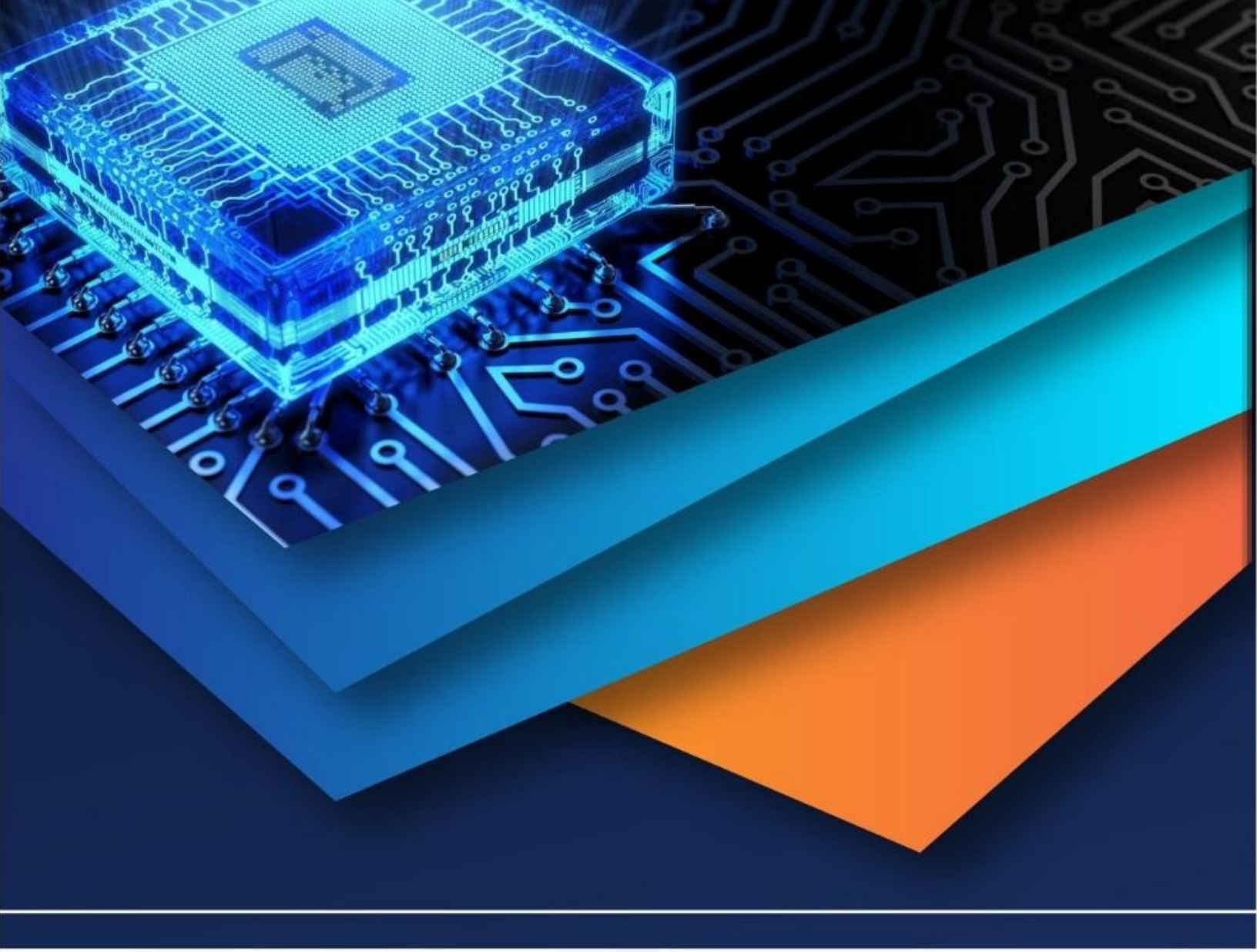
[7] Namasudra S. An improved attribute-based encryptiontechniquetowards the data security in cloud computing. Concurr. Comput. 2019;31(3). doi:10.1002/cpe.4364.

[8] M. Alzain, B. Soh and E. Pardede, "MCDB: Using Multi- Clouds to Ensure Security in Cloud Computing", IEEE conference on Dependable, Autonomic and Secure Computing, December– 2011, pp. 784 – 791.

[9] D. Sureshraj, and V. Bhaskaran, "Automatic DNA Sequence Generation for Secured Cost-effective Multi-Cloud Storage", IEEE Conference on Mobile Application Modeling and Cloud Computing, December – 2012, pp. 1 – 6.

[10] W. Liu, "Research on Cloud Computing Security Problems and Strategy", IEEEE conference on Consumer Electronics, Communications and Networks, April-2012, pp. 1216 – 1219.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)