A New Cryptographic Encryption Approach for Cloud Environment

Mr. Amit Kumar Mishra
Assistant Professor,Department of Computer Engineering
Sri Balaji College of Engineering & Technology, Jaipur

Sarves Kumar Meena
M.Tech Scholar, Department of Computer Engineering
Sri Balaji College of Engineering & Technology, Jaipur
E-mail-> kumarsamee1994@gmail.com

ABSTRACT: Cloud security and trust management are an important issue in the cloud environment. Cloud computing is the result of the evolution of virtualization, service-oriented design, and the widespread adoption of involuntary and utility computing. Today, cloud computing is the fastest growing technical term and captures a global service-oriented market, so cloud computing service providers and cloud computing consumers need to maintain trust between them. In cloud security, if you discuss the security procedures of traditional IT information systems, designing security into cloud software during the software development life cycle can greatly reduce the cloud attack surface. With cloud computing providing Security as a Service (SAAS), security software is an important issue. From a cloud customer perspective, the use of security services in the cloud reduces the need for security software development. The requirements for security software development are transferred to the cloud provider. This work proposes a new cloud environment security and trust management algorithm, which uses the cryptosystem method to improve the single alphabet based on the concept of multi-letter cipher. Encryption and decryption is applied to plain text to encrypt text and cipher text for plain text conversion. In this work, the algorithm's power consumption, encryption and decryption throughput, and security analysis are also presented.

*****

I. Introducation

The Internet is all over the world. The Internet is used for different purposes in different domains. These days, the practical significance of using the Internet is changing. The way people calculate is even more advanced than the type of computer they use. A few days before the Internet, the service was very effective, unlike the current situation. Today, Internet services are constantly being improved to provide services based on user needs. However, systems with limited storage and computing power to run these services are not functional. If the user installs any heavy software or wants better computing performance, he/she is often affected by the inefficient hardware support.

TABLE 1.1
Cloud Computing Timeline

Decade	Characteristics	Notes
1960s	McCarthy‟s concept & other academic research	
1970s	Mainframe timesharing, ARPANET	IBM & the “Seven dwarfs”-
1980s	ARPANET and the emergence of thin client	NeXT, Object Oriented Programming and GUIs
1990s	Hotmail, Salesforce, Peer1 Hosting	SaaS emerging, Net Centric trademark
2000s	Amazon Web Service, Rackspace, DropBox& othersemerge	Cloud Revenue estimated at US$ 58.6
2010s	Google Drive, Amazon Cloud Drive, LG Cloud, icloud, Smartphones	1 new Server added to the cloud for every 600 Smartphones.

Cloud computing solves all of these problems. Cloud computing enables end users to provide users with a better computing experience. Cloud computing is an upgrade to technologies such as parallel computing, distributed computing or grid computing.

1.1 General Overview

The term cloud refers to a combination of computer systems and servers to access services with the help of the Internet. This collection of servers can be controlled and managed by a third party service provider, which can be located anywhere in the world. Cloud computing service providers offer many hosted services that customers frequently request. The National Institute of Standards and Technology (NIST) defines cloud computing, which is a service and deployment model for cloud computing paradigms. Visualization model defined by NIST cloud computing work:

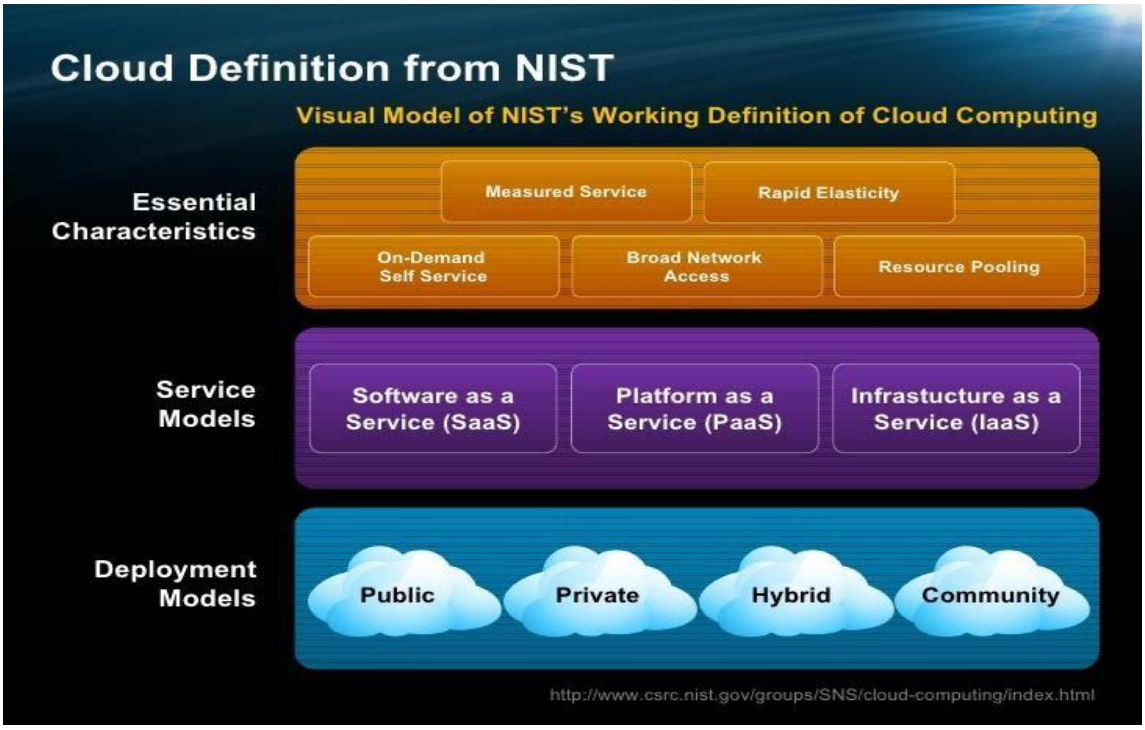
Cloud Definition from NIST
Visual Model of NIST's Working Definition of Cloud Computing
Essential Characteristics
Measured Service
Rapid Elasticity
On-Demand Self Service
Broad Network Access
Resource Pooling
Service Models
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastucture as a Service (IaaS)
Deployment Models
Public
Private
Hybrid
Community
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

Figure 1.1 NIST Visual Model of Cloud Computing Definition

"Cloud computing is an example of providing on-demand network access to shared pools of configurable computing resources (e.g., networks, servers, services, storage, and applications) that can be quickly configured and configured with minimal administrative effort or service provider interaction. Delivery". Cloud computing models offer the benefits of cost savings and more IT usage. It is recommended that the government and industry should start using this technology to cope with difficult economic conditions. Cloud computing is currently used, but its security and interoperability are major obstacles to its widespread use.

1.2 Problem Statement

The primary focus of any organization is security, which is the key to cloud success. As many surveys show, security in cloud and trust management is now a major challenge for cloud computing. Trust is one of the most important parts of the adoption and development of cloud computing. Since cloud computing is widely used in a technology, new problems arise according to their needs. Of serious concern are security, including service availability; data confidentiality and provider lock-in. The basic idea of cloud computing is not new. Cloud computing is not a technological advancement, but a new mode of operation. Therefore, cloud computing is compared to many existing technologies. Due to the nature of cloud computing such as security, a newproblem has arisen.

In previous algorithms, statistics or systems were controlled by third parties. A third party created by a cloud service provider. When users store data in the cloud, they stay in the cloud. Users can't be assured that after the user deletes the data, it will no longer exist anywhere. It observes that the security of stored data is low. In this work, a new encryption-decryption algorithm is proposed, which is superior to previous algorithms for throughput and power consumption and trust as a service. Algorithms already in use do not meet user expectations. In previous algorithms, there were many problems, namely small key size, high execution time for encryption and decryption at different data sizes, low throughput and high power consumption. These algorithms have some of the problems addressed in the proposed algorithm.

In the proposed work, an algorithm was developed. The first algorithm uses a matrix key that is multiplied by a quaternion vector and applied to the product to generate a sequence of symbol functions. This sequence will be used to create three different alternative method models. The algorithm is then considered to be a replacement algorithm that is shared by the sender and receiver using a single key and the password processes the input elements continuously, producing one element at a time. The new encryption algorithm is based on the concept of the Poly letter cipher, which is an improvement over the single alphabet.

II. LITERATURE SURVEY

When delegating key organizational information to a geographically dispersed cloud platform, security is a major issue, not directly controlled by the organization. If we discuss traditional IT information system security procedures, designing security into cloud software during the software development lifecycle can greatly reduce the cloud attack surface. From the perspective of cloud consumers, the use of SAAS in the cloud reduces the need for security software development. The requirements for security software development are transferred to the cloud provider.

Cloud computing is the next generation of technology that provides us with on-demand, reliable, and secure software, applications, and infrastructure as a service. Cloud computing is also known as the fifth utility service, such as water, electricity, and energy.

Trust only works when the environment is uncertain and the risk is high.

- Trust is the basis for making certain decisions.
- Trust is formed using early knowledge, practice and experience.
- Trust is a subjective concept that depends on individual evaluations and values.
- Trust depends on time and new knowledge, and experience has an overriding importance to old knowledge.
- Trust is multifaceted.
- Trust depends on the context.

The accuracy of entity credibility can be accurately estimated based on the results of universal standards in objective trust. If trust is estimated based on personal interests, the resulting trust is called subjective trust. Decisions made based on individual transactions and their outcomes are referred to as transaction-based trust, and trust established depends on the individual's assessment and is based on assessed trust. If the trust build operation requires information from each node, it is called complete information, and it is called a global trust function or a full trust function. If the information obtained only from one neighbor is called the localized information trust function. If an entity's trust ranks from best to worst, then it is based on ranking trust, and does trust depend on it? The predetermined trust threshold is called a threshold-based trust. Once the expected reputation information is found, a backward ant is formed. When the ant returns, it updates all the reputation tables in each node. In this section, we focus on security. As we discussed earlier, security is the primary area of focus in cloud computing. If security is not handled properly, the entire area of cloud computing will fail because cloud computing primarily involves managing sensitive personal information in public networks. In addition, security from service provider points becomes very important in order to protect networks and resources in order to increase the robustness and reliability of these resources. Establishing trust management for trust models of elemental and entity behavior is especially useful for properly managing cloud systems and cloud services. Various research groups in the industry and academia are doing business in the field of trust management in cloud computing.

III. PROPOSED WORK

In the proposed work, the customer or user interacts with a third-party auditor. A third-party auditor is an authorized person designated by the cloud owner (cloud service provider). Then, for the trust as a service, a new research on the security of cloud computing and the research work of designing a new encryption algorithm are proposed to follow the sequence of STEPs.

1. Definition of the problem statement.
2. An algorithm 1 involving multiplication of a quaternary vector matrix of size 256 x 4 and a random matrix of size 4 x 4, and then processing the output of the multiplication operation to generate a secret key. The development of this algorithm involves a process aimed at obtaining the best key.
3. An algorithm 2, the purpose of which is to process plaintext encryption to produce a ciphertext having a key generated in algorithm 1. The ciphertext will follow the transport key, which holds the useful data for the secret key that was decrypted at the receiving end and will be sent along with the cipher text at the end of the sender.
4. Train the developed algorithm with a different key.
5. When sending from the Key Distribution Center, use an appropriate method to identify any garbled key.
6. Comparative analysis of developed algorithms in terms of encryption and decryption throughput as well as power and intensity and security analysis.
7. Work summary and conclusions.

3.1 Problem definition

All encryption algorithms rely on two common principles. The first is replacement, during which each part of the plaintext is mapped to a different part. The second is transposition, during which the elements in the plaintext are rearranged. Most systems require multiple replacement and conversion phases. Technical experts introduced chaos and proliferation. Confusion can be a technique to ensure that ciphertext does not provide clues about plain text, and Diffusion will increase the redundancy of plain text by propagating between rows and columns.

If the sender and receiver use a similar key, the system is called a symmetric key, a single key key, a key key or a typical encryption key. If both the sender and the receiver use different keys, the system is named asymmetric, 2 key or public key encrypted.

The block cipher creates one partial block of input at a time, generating an output block for each input block. The stream cipher processes the input portion continuously, producing a portion at a time as it continues.

3.2 proposed algorithm

The first algorithm uses a matrix key that is multiplied by a quaternion vector and uses a symbol function to produce a sequence on the result. This sequence will be used to create 3 different alternative method models. Therefore, the algorithm is examined as a replacement algorithm that is shared by the sender and receiver using a single key, and the password periodically creates input elements, one at a time. The algorithm developed depends on the concept of the Poly letter cipher, which is an improvement over the single alphabet.

3.2.1 Algorithm for generating sequences

STEP #1. Let a sequence of 0 to N values, where N is a positive integer.

STEP #2. Convert each element of the sequence to a quaternion of the given number number.

STEP #3. The value of STEP#2 is represented in a matrix of 256×4.

STEP#4. Subtract 1 from each element of the matrix defined in STEP#3.

STEP#5. Consider a random matrix key of size (4X4).

STEP#6. The output of STEP#4 is multiplied by the output of STEP#5.

STEP #7. Converts all positive values of the matrix (256 x 4) to 1, converts negative values to -1, and converts zero to zero.

STEP #8. Add 1 to each element of STEP#7 output.

STEP #9. Convert the quaternion value of STEP#8 to decimal form. Generate a sequence.

1.2.2 A New Substitution Cipher Model for Cloud ComputingSecurity

The algorithm that will be discussed in this work will generate a sequence. The algorithm m considers the matrix key and performs a series of STEPs to generate a sequence. Each plaintext block is changed from alphanumeric content of the plain text and the generated sequence to form a ciphertext. Therefore, the ciphertext obtained without knowing the key is computationally infeasible.

3.2.3 Encryption algorithm

STEP#1. Treat any random sequence as plain text.

STEP#2. Calculate the total number of characters in WC.

STEP #3. Convert each element of the sequence to the ASCII equivalent code.

STEP#4. Consider the key sequence we generated in Algorithm 4.3.

STEP#5. Add the ASCII equivalent element in STEP#3 and the key in STEP#4.

STEP#6. The MOD operation is performed on the output of STEP#5, and if the WC is ODD, the Mod64 operation is followed, otherwise Mod 128 is executed.

STEP #7. If the ASCII code is between 0 and 32, and if WC is EVEN then add a prefix and suffix (point, stop ASCII CODE 46 =.), then generate an ASCII equivalent, otherwise use ODD and then add a prefix and suffix (question mark ASCII) CODE 63 =?) Create a ciphertext and transport key from STEP#6.

3.2.4 Decryption algorithm

STEP#1. Consider the cipher text in Algorithm 4.5.1.

STEP#2. Load ASCII Even and ODD tables. Convert each element of the sequence to an ASCII equivalent.

STEP #3. Consider the transport key we generated in Algorithm 3.5.1.

STEP#4. Execute the operation between the ciphertext ASCII equivalent operation we generated in STEP#2 and the transport key in STEP#3.

STEP#5. Generate a key from the transport key.

STEP#6. Between the output of subtraction STEP #4 and the output of STEP #5.

STEP #7. Write the equivalent ASCII code from the ASCII table. We get the decrypted plain text.

3.2.5 Characteristics of the new algorithm

1. Replace the rule with a set of multiple letters.
2. Developed a new block cipher.
3. A random matrix is used for the key.
4. A new coding method.

3.2.6 Advantages of New Algorithm

1. Even if the algorithm is known, generating a matrix key is computationally infeasible.
2. User Diversification: Different users of the Internet can use different modified versions of the new algorithm. Since the sign function is used in the algorithm, it should be powerful enough.
3. According to the matrix, the same characters are replaced by different alphanumeric values, which provide more security for the letters.

3.2.7 Complexity of the New algorithm

Complexity can also be expressed in the order of magnitude. If the length of the key is k, the complexity is expressed as 2k. It shows that 2k operations are required to break the algorithm. In the proposed algorithm, a matrix key is used. The matrix key is multiplied by a quaternion vector. On the generated value, apply the symbol function to change all positive values to 1, change the negative value to -1, and change zero to 0. This represents the basic strength of the algorithm. It is therefore recognized that the algorithm, known ciphertext text, is difficult to create a matrix key. In this algorithm, in addition to trying all key combinations, there is no way to identify the key, and the complexity of the algorithm is considered to be an index of quality.

3.3 Security Analysis

The model uses a symbol function to generate a sequence on the product of the quaternion vector and the matrix key. The sign function changes all positive values to 1, changes negative values to -1, and zeros to 0. This sequence is used for plain text to create cipher text. Therefore, it is difficult to create a matrix key from known plain text and ciphertext. So this model there is no differential encryption analysis. But this model uses a simple alternative to generate ciphertext; linear cryptanalysis has certain risks. The key cannot be obtained and the entire information is not available, but some information can be obtained in this model. The algorithm is completely unaffected by ciphertext and attack types. Keys may not be recognized by different attacks. In this work, a four-digit quaternary system was used. The key generated therefore is 44, which is 256 digits. By considering a quaternion vector with five or six digits, the length of the key can be increased by 45, 46, which improves the length of the created key. Therefore, by considering the n-ary vector, the length of the created key can still be increased. Therefore, by increasing the length of the key, the security of the cryptosystem can be further improved.

IV. IMPLEMENTATION & RESULT

Cloud computing is a key technology in today's world. The technology is undergoing extensive research. Despite this research, there are some aspects as most organizations and cloud customers are less confident in entering this new paradigm called cloud. Therefore, from a security perspective, all existing systems are not as reliable. We compare our proposed algorithm with other existing algorithms based on some parameters. To prove that our proposed work is more efficient than other work, we introduced a new encryption technology that reduces the execution time of encryption and decryption. It also provides high throughput and low power consumption as well as increased security.

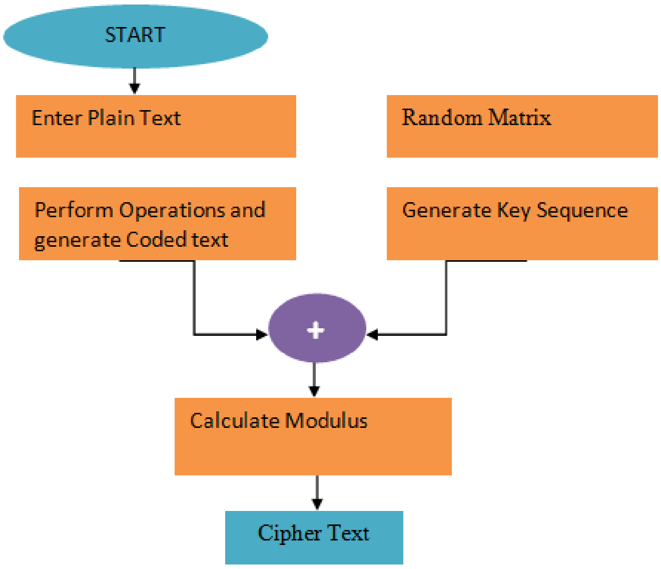

Figure 4.1 Data Flow Diagram

In Figure 4.1, first enter plain text, then perform operations on plain text and generate encoded text.

- Create a key sequence along with this generated random matrix.
- Calculate the resulting modulus of the above STEPs and finally generate a ciphertext.

4.1 Comparative Analysis

In this part, we compare our work with other existing technologies. We represent our results in the context of different parameters, for example:

1. Calculate the execution time of different input sizes for encryption and decryption.
2. Calculate the throughput and power consumption of various algorithms.
3. Security analysis.

In Table 4.1, we calculated the execution time (in milliseconds) for different input data sizes, such as 49 kbytes, 59 kbytes, 100 kbytes, 247 kbytes, 321 kbytes, 694 kbytes, and 899 kbytes.

After analyzing this output 10 times for each input size data, we calculated the average time for each input size. Then we calculated the average time for all input size data, which is the execution time (in milliseconds) we used for encryption.

TABLE 4.1

Calculate Execution Time (msec) For Encryption

S. No.	**Execution Time (msec) For Encryption**						
	49 kbytes	**59 Kbytes**	**100 Kbytes**	**247 kbytes**	**321 kbytes**	**694 kbytes**	**899 Kbytes**
1	10	10	20	60	80	170	260
2	10	10	20	60	80	160	220
3	10	10	20	50	70	180	290
4	10	10	20	50	80	170	280
5	10	10	20	60	70	160	230
6	10	10	20	50	70	170	250
7	10	10	20	60	70	180	260
8	10	10	20	60	70	170	250
9	10	10	20	60	70	160	250
10	10	10	20	60	80	170	220
Average	**10**	**10**	**20**	**57**	**74**	**169**	**251**
Average Total Time (msec)	**84.42 (msec)**						

In Table 4.2, we calculated the execution time (in milliseconds) for different input data sizes, such as 49 kilobytes, 59 kilobytes, 100 kilobytes, 247 kilobytes, 321 kilobytes, 694 thousand Bytes and 899 kilobytes.

After analyzing this output 10 times for each input size data, we calculated the average time for each input size.
Then we calculate the average time for all input size data, which is the execution time (in milliseconds) we used for decryption.

TABLE 4.2

Calculate Execution Time (msec) For Decryption

S.No.	**Execution Time (msec) For Decryption**						
	49 kbytes	**59 kbytes**	**100 kbytes**	**247 kbytes**	**321 kbytes**	**694 kbytes**	**899 kbytes**
1	10	10	20	60	90	90	200
2	10	10	20	50	80	160	100
3	10	10	20	70	80	150	170
4	10	10	20	80	70	180	180
5	10	10	20	60	90	160	230
6	10	10	20	80	90	100	210
7	10	10	20	70	70	160	210
8	10	10	20	70	70	150	220
9	10	10	20	60	70	150	210
10	10	10	20	80	80	160	190
Average	**10**	**10**	**20**	**68**	**79**	**146**	**192**
Average Total Time (msec)	**75 (msec)**						

In Table 4.3, the execution time of the encryption is used to calculate the throughput of the encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated by dividing the encrypted megabyte total plaintext by the total encryption time (in milliseconds) of each algorithm. As the throughput value increases, the power consumption of encryption technology decreases.

- Encrypted throughput (megabytes per second) = _______________
- Throughput ___________________
- Encrypted throughput in the proposed algorithm = 3.9145 megabytes per second
- The encryption throughput in the proposed algorithm is higher compared to DES and AES. Therefore the proposed algorithm is better.

TABLE 4.3

Throughput Analysis between Different Algorithms for Encryption [30]

Input size in (kbytes)	DES (msec)	AES (msec)	Proposed (msec)
49	29	54	10
59	33	48	10
100	49	81	20
247	47	111	57
321	82	167	74
694	144	226	169
899	240	299	251
Average Time	89.1	140.86	84.42
Throughput (Megabytes/sec)	**3.7074**	**4.3463**	**4.9145**

In Fig 4.2 we have explained throughput of DES, AES and PROPOSED algorithms with the help of bargraph.

As a result, encryption time for proposed algorithm is better than DES and AES.

Less power consumption in proposed algorithm compared to DES and AES.

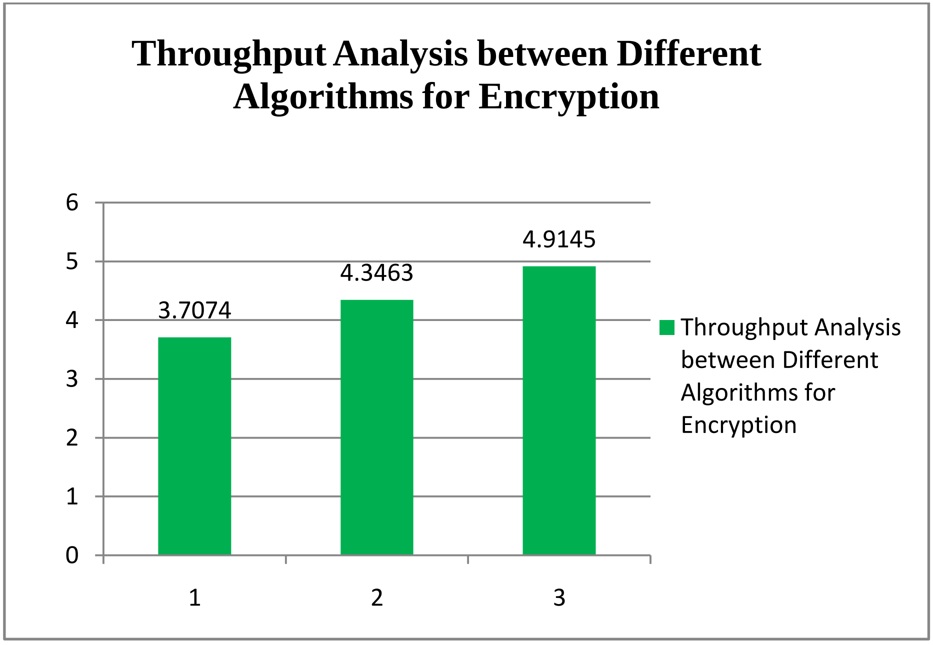

Figure 4.2 Bar Graph for Throughput in different Algorithm for Encryption

In Table 4.4, the throughput of the Decryption scheme is calculated similarly as in encryption, it indicates the speed of Decryption.

- Throughput For Decryption In Proposed Algorithm = 4.7066Megabytes/sec

TABLE 4.4

Throughput Analysis between Different Algorithms for Decryption [30]

Input size in (kbytes)	DES (msec)	AES (msec)	Proposed (msec)
49	50	53	10
59	42	51	10
100	57	57	20
247	72	77	68
321	74	87	79
694	120	147	146
899	152	171	192
Average Time	81	91.86	75
Throughput (Megabytes/sec)	**4.0802**	**4.5978**	**4.7066**

In Fig 4.3 we have explained throughput of DES, AES and PROPOSED algorithms with the help of bargraph. As a result, decryption time for proposed algorithm is better than DES and AES.Less power consumption in proposed algorithm compared to DES and AES.

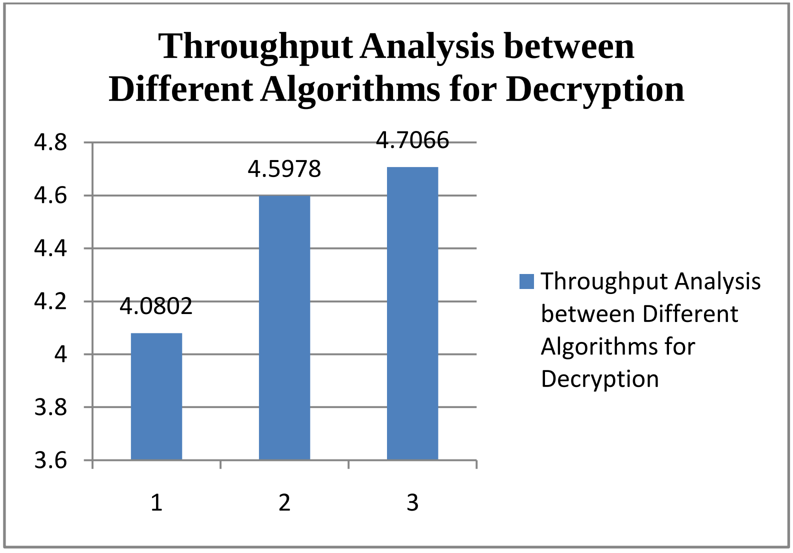

Figure 4.3 Bar Graph for Throughput in different Algorithm for Decryption

DES encrypts data in 64-bit block sizes and works efficiently with 56-bit keys. The 56-bit key space has a probability of approximately 72 peta flops. It looks great, but based on today's computing power, it is not enough and vulnerable to brute force attacks. Therefore, DES can't keep up with the advancement of technology; it is no longer related to security. Since DES was widely used at the time, Advanced Encryption Standard (AES) , is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES encrypt the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. Brute force attack is the only effective attack known against this algorithm. AES encryption is fast and flexible

TABLE 4.5
Comparison with existing algorithms

S.No.	FACTORS	DES	AES	PROPOSED
1	KEY LENGTH	56 BITS	128, 192 or 256 BITS	256 BYTE
2	CIPHER TYPE	SYMMETRIC ALGORITHM 🟥🟦	SYMMETRIC BLOCK CIPHER 🟩	SYMMETRIC ALGORITHM
3	BLOCK SIZE	64 BITS	128, 192 or 256 BITS	256 BYTE
4	DEVELOPED	1977	2000	2018
5	KEY	SINGLE	SINGLE	SINGLE
6	POSSIBLE KEYS	2^{56}	2^{128}, 2^{192}, 2^{256}	2^{256x8}
7	THROUGHPUT (MB/sec) (Encryption/Decryption)	3.7074/4.0802	4.3463/4.5978	4.9145/4.7066
8	SECURITY	PROVEN INADEQUATE	SECURE	SECURE
9	ROUND	16	10(128-bits),12(192-bits),14(256-bits)	1

Since DES and AES have proven inadequate in providing security and handling today's computing power, our algorithmic encryption and decryption seems to be more reliable because the key length is increased and therefore the possible keys are increased. DES, AES and our proposed algorithm are symmetric algorithms that use the same key for encryption and decryption. The throughput in the observed algorithm is improved over existing algorithms. Since throughput is inversely proportional to power consumption, power consumption decreases as throughput increases.

4.3 Computing Power Analysis

The total number of calculations required to convert plain text to ciphertext.

Calculation 1: Convert n = 0:255 to a quaternion vector. Let it be QVR.

Calculation 2: Calculate QVR-1 and store it in QVR**.**

Calculation3: Multiply QVR by the key considered.

Calculation 4: Apply the symbol function to the product. Store it in QVR.

Calculation 5: Calculate QVR + 1.

Calculation 6: Convert the output quaternion vector to an integer form. This was designated as SEQ to generate a sequence.

Calculation 7: Convert plain text to ASCII.

Calculation 8: Add the ASCII value of plain text to the generated sequence.

Calculation 9: Apply the mod function on the output.

Calculation 10: Convert the output to characters in the alphabet to get the ciphertext. Therefore, the total number of calculations in the first proposed model is 10.

The computational overhead (computing power) of a 256-character key. First calculation: 256 calculations, Second calculation: 256 calculations. Key to consider: character key, 3rd calculation: 256 x 16 calculation,

The fourth calculation: 256 calculations, the fifth calculation: 256 calculations, the sixth calculation: 256 calculations,

The seventh calculation: 256 calculations. Consider 256 characters of plain text, 8th calculation: 256 calculations,

The ninth calculation: 256 calculations, the 10th calculation: 256 calculations.

Therefore, the total computational cost of the model is 6,400 calculations.

4.4 Complexity of the Model

I calculation: convert n = 0: 256 into a quaternion vector. Let it be QVR. Complexity is a multiple of n.

II calculation: Calculate QVR-1. Complexity is a multiple of n.

III Calculation: Multiply the QVR by the key considered. Complexity is a multiple of n

IV calculation: Apply the signature function on the product. Store it in QVR. Complexity is a multiple of n

V calculation: Calculate QVR + 1. Complexity is a multiple of n

VI calculation: Convert the output quaternion vector to an integer form. This was designated as SEQ to generate a sequence. Complexity is a multiple of n

VII Calculation: Convert plain text to ASCII values. Complexity is a multiple of n

VIII Calculation: Add the ASCII value of plain text to the generated sequence. Complexity is a multiple of n

IX calculation: Apply the mod function on the output. Complexity is a multiple of n

X calculation: Convert the output to the characters of the alphabet to get the ciphertext. Complexity is a multiple of n.

Therefore, we can say that the complexity of the model is O(n).

V. CONCLUSION

Finally, we are at the end of this study. We focus on this research on cloud computing security and trust management between cloud service providers and cloud customers. This study represents the importance of the encryption and decryption phases used in cloud security. Given the rapid development and globalization of communications, the importance of encrypted data can be identified. The advantage of encrypting data in the cloud keeps the trust between cloud customers because they want to show security and confidentiality in real-time applications. Data encryption is of particular importance in applications such as e-mail, e-commerce, electronic cash, etc., where highly vulnerable communication lines are accessed to transmit highly variable data.

The encryption model introduced in describes the new block cipher technology. The algorithm considers the matrix key and performs a series of STEPs to generate another sequence. This model is a new symmetric encryption technique. In this model, it is observed that for a given key, the total computational overhead is 1600 calculations. The complexity of the model constructed from it is O (n) of its strength, which is exponential in nature. Compared to other algorithms, the throughput is much better, so the power consumption is very low. It has also been observed that many variations in the cryptographic text are identified by slight changes in the key, which provides more strength to the generated algorithm. The algorithm is completely immune to attacks on ciphertext.

In this work, a four-digit quaternary system was used. So the generated key is 44, which is 256 digits. By considering a quaternion vector with five or six digits, the length of the secret key can be increased by 45, 46, which increases the length of the generated key. Similarly, by considering the n-ary vector, the length of the generated secret key can still be increased. Therefore, by increasing the length of the key, the security of the cryptosystem can be further improved.

Current work involves plain text in alphanumeric characters and characters. This work can be improved so that it can support not only English but also characters in other languages. It can also improve the work, not only supporting text, but also other forms of message transmission, such as audio, video and images. We will analyze the performance of other algorithms in terms of throughput and power consumption.

REFERENCES

[1] R. Buyya, C. Shin Yeo, J. Broberg, and I. Brandic, “Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Computing System, vol. 25, pp. 599–616,2009.

[2] Web Reference fromhttp://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[3] Ronald L. Krutz, Russell Dean Vines,"Cloud Security: A Comprehensive Guide to Secure Cloud Computing", ISBN: 978-0-470-58987-8, Wiley Publishing,Inc.

[4] William Stallings, “Cryptography and Network Security Principles and Practice”, ISBN 978-9332518773, Pearson Education India, 6th edition.

[5] Khaled M Khan and QutaibahMalluhi, "Establishing Trust in Cloud Computing," IT Professional, vol. 12, no. 5, pp. 20 - 27,2010.

[6] Zhexuan Song, Jusus Molina, and Christina Strong, "Trusted Anonymous Execution: A Model to Raise Trust in Cloud," in 9th International Conference on Grid and Cooperative Computing (GCC), Nanjing, China, 2010, pp. 133 -138.

[7] Hiroyuki Sato, Atsushi Kanai, and ShigeakiTanimoto, "A Cloud Trust Model in a Security Aware Cloud," in 10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT), Seoul, South Korea, 2010, pp. 121 -124.

[8] Wenjuan Li, Lingdi Ping, and Xuezeng Pan, "Use trust management module to achieve effective security mechanisms in cloud environment," in International Conference on Electronics and Information Engineering (ICEIE), vol. 1, Kyoto, Japan, 2010, pp. 14- 19.

[9] Tie Fang Wang, Bao Sheng Ye, Yun Wen Li, and Yi Yang, "Family Gene based Cloud Trust Model," in International Conference on Educational and Network Technology (ICENT), Qinhuangdao, China, 2010, pp. 540 -544.

[10] Tie Fang Wang, Bao Sheng Ye, Yun Wen Li, and Li Shang Zhu, "Study on Enhancing Performance of Cloud Trust Model with Family Gene Technology," in 3rdIEEE International Conference on Computer Science and Information Technology (ICCSIT), vol. 9, Chengdu, China, 2010, pp. 122 -126.

[11] Paul D Manuel, ThamaraiSelve, and Mostafa Ibrahim Abd-EI Barr, "Trust management system for grid and cloud resources," in First International Conference on Advanced Computing (ICAC 2009), Chennai, India,2009, pp. 176-181.

[12] ZhidongShen, Li Li, Fei Yan, and Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform," in International Conference on Intelligent Computation Technology and Automation (ICICTA), vol. 1,Changsha, China, 2010, pp. 942 -945.

[13] ZhidongShen and Qiang Tong, "The security of cloud computing system enabled by trusted computing technology," in 2nd International Conference on Signal Processing Systems (ICSPS), vol. 2, Dalian, China, 2010, pp.11-15.

[14] Mohammed Alhamad, Tharam Dillon, and Elizabeth Chang, "SLA-based Trust Model for Cloud Computing," in 13th International Conference on Network-Based Information Systems, Takayama, Japan, 2010, pp. 321-324.

[15] Xiao Yong Li, Li Tao Zhou, Yong Shi, and Yu Guo, "A trusted computing environment model in cloud architecture," in Ninth International Conference on Machine Learning and Cybernetics (ICMLC), vol. 6, Qingdao, China,2010, pp.2843-2848.

[16] Zhimin Yang, LixiangQiao, Chang Liu, Chi Yang, and Guangming Wan, "A CollFaborative Trust Model of Firewall-through based on Cloud Computing," in 14th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Shanghai, China, 2010, pp. 329 -334.

[17] Junning Fu, Chaokun Wang, Zhiwei Yu, Jianmin Wang, and JiaGuang Sun, "A Watermark-Aware Trusted Running Environment for Software Clouds," in Fifth Annual China Grid Conference (China Grid), Guangzhou, China,2010, pp. 144 -151.

[18] RohitRanchal et al., "Protection of Identity Information in Cloud Computing without Trusted Third Party," in 29th IEEE International Symposium on Reliable Distributed Systems, New Delhi, India, 2010, pp. 1060-9857.

[19] Hassan Takabi, James B.D Joshi, and Gail JoonAhn, "Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," in 34th Annual IEEE Computer Software and Applications Conference Workshops, Seoul, South Korea, 2010, pp. 393 -398.

[20] Web reference fromhttps://en.wikipedia.org/wiki/DataEncryptionStandard.

[21] AtulKahate, “Cryptography and Network Security”, ISBN 1-25-902988-3, McGraw Hill Education (India) Private Limited, 3rdedition.

[22] Sombir Singh, Sunil K.Makkar and Dr.Mukesh Kumar, "Enhancing the Security of DES Algorithm Using

Transposition Cryptography Techniques" in IJARCSSE in volume 3, issue 6,BRCM CET, Bahal, India 2013, ISSN: 2277 128X.

[23] Des encryption by National Institute of Standards and Technology (NIST) chapter6.

[24] Li, J., Li, B., Meng, L., & Sun, D, “HiTrust: A hybrid tree based trust negotiation service” IEEE 24th International Conference on Advanced Information Networking and Application Workshops, 2010.doi:10.1109/WAINA.2010.149.

[25] Kramer, S., Gore, R., & Okamoto, E,“Formal dentitions and complexity results for trust relations and trust domains” March2012, from http://www1.spms.ntu.edu.sg/ccrg/documents/trust.pdf.

[26] Abawajy, J,”Determining service trustworthiness in inter cloud computing environments”. 10th International Symposium on Pervasive Systems, Algorithms,and Networks,2009,doi:10.1109/I-SPAN.2009.155.

[27] Habib, M. H., Reis, S., &Muhlhauser, M,“Towards a trust management system for cloud computing” International joint conference of IEEETrustCom-11/IEEE ICESS-11/FCST-11, 2011,doi:10.1109/TrustCon.2011.129.

[28] Skogsrud, H. &Benatallah, B,“Model-driven trust negotiation for web services. IEEE Internet Computing”.2003, doi:10.1109/MIC.2003.1250583.

[29] Kerr, R. & Cohen, R, “Smart cheaters do prosper: Defeating trust and reputation systems.”, 8th International Conference on Autonomous Agentsand

[30] MultiagentSystems,March 2012, from www.cs.uwaterloo.ca/rckerr/KerrCohenaamas2009draft.pdf.

[31] MilindMathur and Ayush, “Comparison Between DES , 3DES , RC2 , RC6 , BLOWFISH AND AES “, National Conference on New Horizons inIT,2013.

[32] G. Ramesh and R. Umarani,”A Comparative Study of Six Most Common Symmetric Encryption Algorithms across Different Platforms “, International journal of Computer Application, ISSN: 0975 – 8887, Volume 46– No.13, May 2012.

[33] SaketMaskara1, MuditSaraf and Priya G,”Trust Management in Cloud Computing”, International Research Journal of Engineering and Technology,ISSN: 2395-0072, Volume: 03 Issue: 11, Nov -2016.

[34] R.GowthamiSaranya and A.Kousalya,”A Comparative Analysis of Security Algorithms Using Cryptographic Techniques in Cloud Computing”, International Journal of Computer Science and Information Technologies, ISSN: 0975-9646, Vol. 8 (2), 2017, 306-310.