Research Article

A Review Study on Security Issues, Benefits, Risks and Various Challenges in Cloud Computing Platform and Proposed Model for Enhancing Security for Sensitive Data

Prof.N.Krishnamoorthy[a], Dr.S.Umarani[b], and M.Dhivya[c]

[a,c] Assistant Professor -Department of Computer Applications -SRM Institute of Science and Technology, Ramapuram, Chennai-600 089(Erstwhile SRM University)

[b]Professor and Head-Department of Computer Science-SRM Institute of Science and Technology, Ramapuram, Chennai-600 089(Erstwhile SRM University)

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

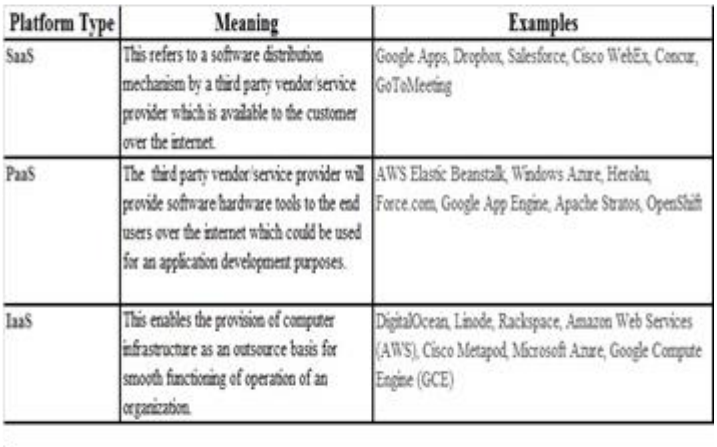
Abstract: In this recent and technological epoch, Cloud Computing(CC) is the generally promising and upcoming trend in the Universe which aims at the high performance supercomputing. It is the on-request openness of computer system assets, in particular storage space and computing supremacy, with no forthright dynamic supervision by the user. The expression is by and large used to illustrate Data Centers (DC) available to many users over the Internet. Nowadays, most of the organizations move into cloud because it helps the end users to store their personal data into the cloud which can be accessed by the user at anytime and anywhere across the globe. The users data is stored and maintained in DC of the cloud providers viz.. Google, Amazon, Microsoft etc. Despite several advantages of using the cloud computing technology, the end users hesitate to utilize the various cloud services and business organizations are unwilling to deploy/set up their businesses in the cloud because of several security threats and issues involved in cloud computing. The main emphasis of our study shall discuss the cloud computing technology , its characteristics, deployment models, service models and the various security issues, challenges related to cloud computing. We shall also present a schematic idea/algorithm which could be used to ensure the security of sensitive data in cloud storage.

Keywords: cloud computing, Data Centers(DC), benefits, risks.

1. Introduction

CC is defined as a methodology of securely storing our information with the help of bundles of servers deployed on the Internet to accumulate, handle, and process data, instead on a local server or a own gadget. It is composed of a 3-4-5 combination: Three service models - Four deployment models –Five essential characteristics. [1]

Three Service Models



Platform Type	Meaning	Examples
SaaS	This refers to a software distribution mechanism by a third party vendor/service provider which is available to the customer over the internet.	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
PaaS	The third party vendor/service provider will provide software/hardware tools to the end users over the internet which could be used for an application development purposes.	AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift
IaaS	This enables the provision of computer infrastructure as an outsource basis for smooth functioning of operation of an organization.	DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

Table 1: Cloud Service Models -Examples

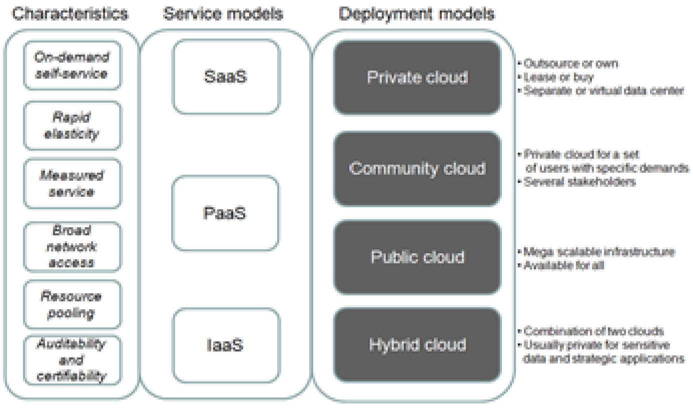


Figure1: Cloud characteristics

Four styles of Cloud operation form

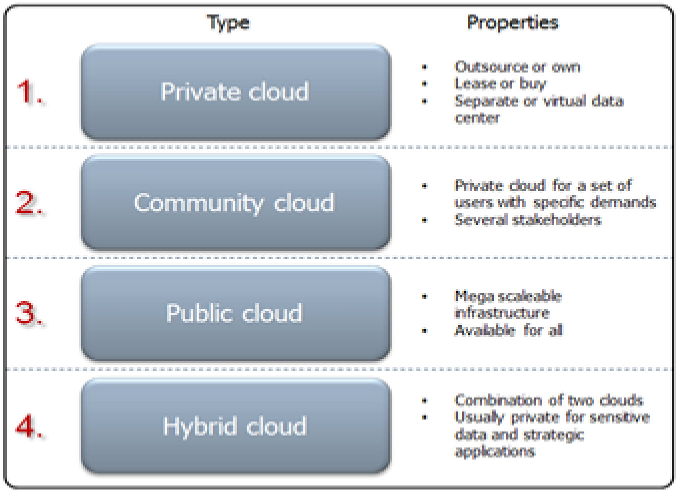

Type
Properties
1.
Private cloud
• Outsource or own
• Lease or buy
• Separate or virtual data center
2.
Community cloud
• Private cloud for a set of users with specific demands
• Several stakeholders
3.
Public cloud
• Mega scaleable infrastructure
• Available for all
4.
Hybrid cloud
• Combination of two clouds
• Usually private for sensitive data and strategic applications

Figure 2: Cloud Deployment Models

Five Characteristics

i. a la carte self-service: One can easily use the various CC holdings without any human intervention

ii. Broad network access: The various CC resources could easily be accessed with the help of any gadgets.

iii. Resource pooling: The cloud resources could be simultaneously accessed by more number of customers (multi tenancy).

iv. Rapid elasticity: The CC resources shall be easily scaled up or scaled down based on-demand.

v. Measured service: Cloud systems routinely manage and upgrade resource use by implementing pay as you use.

2. A Range of Protection Concerns And Threats In CC

As of now, we can see that the great difficulty in cloud computing technology is to demystify the various issues associated with cloud deployment. However these issues arise due to the problem of an architecture issue in which a single instance of a software application serves multiple customers. From the above diagram3, we can understand that from the perspectives of users and an organization that how the security and privacy issues are to be handled efficiently.

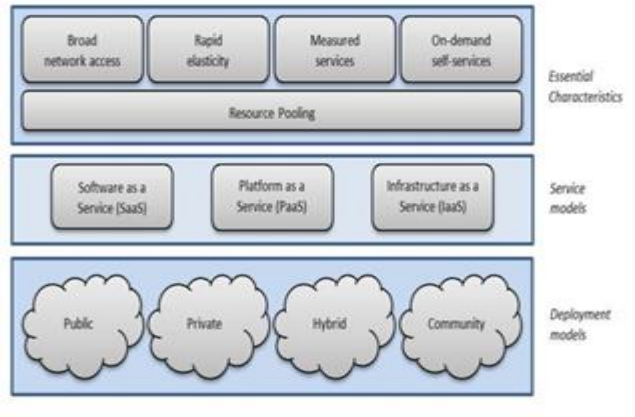


Figure 3: Cloud Computing visual model

There are about six common security issues associated with cloud computing [2]

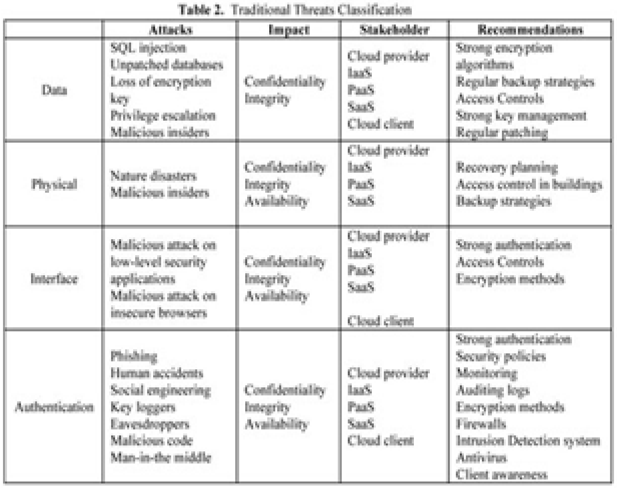


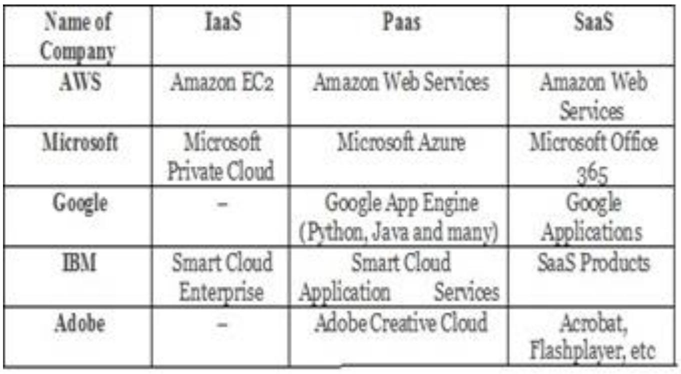
Table 2. Traditional Threats Classification

	Attacks	Impact	Stakeholder	Recommendations
Data	SQL injection Unpatched databases Loss of encryption key Privilege escalation Malicious insiders	Confidentiality Integrity	Cloud provider IaaS PaaS SaaS Cloud client	Strong encryption algorithms Regular backup strategies Access Controls Strong key management Regular patching
Physical	Nature disasters Malicious insiders	Confidentiality Integrity Availability	Cloud provider IaaS PaaS SaaS	Recovery planning Access control in buildings Backup strategies
Interface	Malicious attack on low-level security applications Malicious attack on insecure browsers	Confidentiality Integrity Availability	Cloud provider IaaS PaaS SaaS Cloud client	Strong authentication Access Controls Encryption methods
Authentication	Phishing Human accidents Social engineering Key loggers Eavesdroppers Malicious code Man-in-the middle	Confidentiality Integrity Availability	Cloud provider IaaS PaaS SaaS Cloud client	Strong authentication Security policies Monitoring Auditing logs Encryption methods Firewalls Intrusion Detection system Antivirus Client awareness

1. DDoS -Normally in a cloud environment, the possibility of DDoS attacks is very high since more number of devices would have access to the cloud which will cause the CC system to tear off.
2. Shared Cloud Computing Services-Usually when dealing with shared resources, there is a possibility that, due to lack of security for participating clients, threats can come from/to one participating client to the other , which will create a situation where security for a client is not ensured and would be a threat.
3. Employee Negligence-In this modern era, the intentional and unintentional negligence from employees and various mistakes committed by them leads to a bottleneck with respect to cloud security.
4. Data loss and inadequate data backups- Ransomware prevent accessing an information prior to a ransom is compensated.
5. Phishing attacks-The nature of CC is open, phishing has become a common issue. By suing the login credentials of a user, an intruder can easily attack the system and a compromise in this regard would reveal the entire system to the intruder
6. System Vulnerabilities -A computer vulnerability states that a breach in the system can lead to a open attack. It happens due to any kind of weakness present in the system itself. These vulnerabilities be used against an individual and an organization

3. Cloud Security Threats- Current Scenario

The growth of cloud computing has become unimaginable due to its overwhelming response in the society . The table below summarizes some of the services provided by the famous CSP's across the globe.



Name of Company	IaaS	Paas	SaaS
AWS	Amazon EC2	Amazon Web Services	Amazon Web Services
Microsoft	Microsoft Private Cloud	Microsoft Azure	Microsoft Office 365
Google	–	Google App Engine (Python, Java and many)	Google Applications
IBM	Smart Cloud Enterprise	Smart Cloud Application Services	SaaS Products
Adobe	–	Adobe Creative Cloud	Acrobat, Flashplayer, etc

Table 3: Services Provided by Cloud Providers

Figure 4 summarizes the top security threats in cloud computing. The numbers of service providers increases day by day as well as possible security threats. As a result of this huge volumes of data flow into the cloud and in public cloud areas and these areas are of targets for intruders and hackers. [3] .So there is so much of sensitive data available which leads to potential risk. However, the accountability of securing an organization's data in the cloud is the sole responsibility of the customer and not lies with the service provider.

As per the statement from CSA [4], Article issued on 08/08/2018, describes the Top Threats to CC: We can also see the top intimidation to CC (2016).[5]

As per the analysis [4], there are various levels of security breaches identified in famous social media and other applications like: LinkedIn , MongoDB ,Dirty Cow, Zynga & Yahoo

As we refer the results of a appraisal conducted by CSA with industry domain specialist to ascertain the top issues in CC, based on the opinions given by the industry experts. Here we present the top 12 major security concerns in cloud computing based on the survey conducted by CSA by relating the nature of on-demand service and sharing in CC, and are classified according to the line up of sternness.

Data Breaches-It is the situation arising due to human error, weakness in applications or even due to poor security policies in practice. Figure 4: A summary of cloud security threats -CSA survey

Inadequate uniqueness, Credential and right to use administration-Unauthorized users impersonating as genuine persons can study /amend/remove data and reports

Insecure Interfaces and APIs-Usually the CC service providers provides lot of APIs which in turn could be used by the cloud users to interact with the cloud and utilize the cloud services.

System Vulnerabilities-These are utilizable bugs in programs used by unathorized persons to gain access to a system for the aiming at pinching data, have a complete control over the system or troublemaking. Account Hijacking- We have been seeing the concept of account hijacking is done where by means of pishing, malicious exploitation of software vulnerabilities and fraud - leads to intensification of security.

Malicious Insiders- This is due to malicious insiders in the company.

Advanced Persistent Threats (APTs)- It is an attack that infiltrate systems to create a grip in the assets of target organizations for Stealing data .

Data loss- Data placed can be vanished for various motives apart from malevolent assail.

Inadequate carefulness- While we produce trade tactics, cloud methodologies and CSP must be given significance.

Misuse and immoral use of CS-In recent scenario, as per CSA, we can see free cloud services trials, poorly secured cloud deployments, and most usually the fake account sign ups through payment instrument scam depicts various CC representations to malevolent attacks. We could figure out few examples for abuse of cloud based resources like

A. Email spam
B. Phishing crusade
C. Large scale automated click fraud
D. Brute force attacks
E. DDoS attacks

DoS-It is intended to thwart individuals from manipulating their data.

Shared Technology Vulnerabilities- The CSP bring their services by allotting infrastructure, platforms or applications.

4. Literature review

As we can see from the above findings, there are more number of cloud security issues related to different types of technologies like networks, databases, OS, resource arrangement, concurrency regulation & memory supervision [6].

Sumithra R et.al [7] has surveyed the security problems on the IDA encryption algorithm. He compares with the most prominent and well behaved encryption algorithms.

Rohitbhaduria et.al [8] surveyed a details analysis of the copious unanswered areas bullying the cloud computing and affecting the various users.

Anjali V. Almale et.al [9] surveys data mining in cloud computing. Some key features are used for distribution of data in some ways that is understood by user. It proposes to implement cloud security aspects for data mining in cloud system.

Kajal Rani et.al [10] projected an approach to defeat the problems of habitual data defence algorithm and elevating the security of data in cloud computing using steganography, encryption decryption , compression and splitting .

Katarzynakapusta [11] proposed fast breakup method for data shelter in heterogeneous cloud atmosphere. They performed an pragmatic security investigation on data sets of large organizations and results gives good protection. This scheme also performs twice faster than previous fragmentation techniques. Maragoni et al.[12] discussed several issues of cloud secrity.

Savita.A. Harkude& Dr. G.N.KodandaRamaiah discusses on the comparison of the three algorithms[13].

- GZIPSTREAM AND DEFLATE ALGORITHM
- DA ENCRYPTION ALGORITHM
- FAST FRAGMENTATION ALGORITHM

Nadiah M. Almutairy et.al [14] -In their study, they have reviewed some solutions and mitigation methods for improving the security of cloud virtualization systems.

5. Problem Domain

Significance of the Research crisis: Trouble in cloud security

There are three basic issues to be addressed in connection with the cryptographic terms of CC security

Confidentiality, Integrity & Availability.

A. Availability

Timely Availability of sensitive data is one of the most essential security issues in cloud computing due to its dominant effect on cloud-based businesses operations. Let us consider a situation where the CSP/or a cloud server could not provide the data on time to its end user or a business organization, then that end user or business organization is totally out of cloud services and could not operate further and is not eligible to operate properly.

B. Integrity

Data integrity is the guarantee that the data in transit is unspoiled and can only be accessed or modified by those who are actually authorized to do so. To defend further, it is not be malformed in passage and steps have to be there to guarantee that data cannot be changed by an unofficial individual.

C. Confidentiality

Confidentiality refers to the avoidance of the unconstitutional access of the data and consequently making sure that only the user who has the permission can access the data.

6. RELATED WORK

RamalingamSugumar et.al [16] have discussed a one way encryption method. K. Arul Marie Joycee et.al [17] have discussed about Rail fence Transposition Technique to provide a one way encryption and decryption.

The prime objective of this work is to introduce a scheme that can aid to encrypt and decrypt algorithm. The concealment algorithm is also christened as the encryption and decryption algorithm. This method uses DES and RSA algorithm to make encryption when an end user uploads the files in cloud storage, and opposite DES and RSA algorithm to create decryption.

7. Proposed Model/Algorithm For Enhancing Security

The RSA algorithm is cryptographic algorithm, comprise of Public and Private Key. In CC, data is Encrypted by Public–Key and Decrypted with Private-Key.[15]

It is a three stage practice.

1. Key creation
2. Encryption
3. Decryption

1. Key Generation: The foremost action is key creation. It should be completed prior to stage 2.

2. Encryption: is the progression of converting actual information/understandable (Plain Text) into (cipher Text) which is scribbled.

3. Decryption: Practice of changing Unreadable information (Cipher Text) into (plain Text) readable information.

TRANSPOSITION CIPHER / RAIL FENCE CIPHER ALGORITHM COMBINED WITH AES SHIFT KEY AND MIX COLUMNS ALGORITHM

Here we shall consider a two way encryption and the corresponding two way decryption process respectively. Initially we encrypt the text under consideration by means of rail fence transposition algorithm.

The result of this is further encrypted for the second time using AES algorithm shift rows and mix column methodology.

During decryption, the cipher text obtained from the above process shall be decrypted initially with AES algorithm shift rows and mix column methodology followed by rail fence transposition algorithm.

Columnar Transposition Cipher

Given a plain-text message and a numeric key, cipher/decipher the given text using Columnar Transposition Cipher which involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one.

The Encryption process using Rail Fence Cipher and AES Shift Rows & Mix column method

For example

Encryption

Input :SRMIST All The Best

Key = HACK

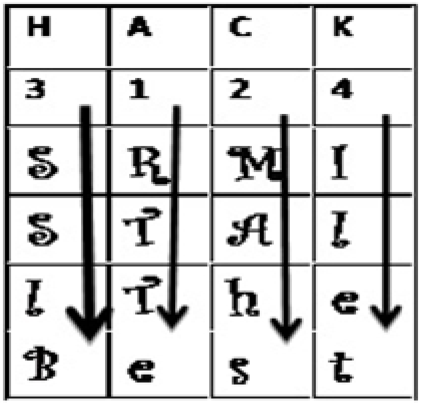
Output :RTTeMAhsSSlBIlet

Decryption

Input :RTTeMAhsSSlBIlet

Key = HACK

Output : SRMIST All The Best



H	A	C	K
3	1	2	4
S	R	M	I
S	T	A	l
l	T	h	e
B	e	s	t

This output/encrypted text is further encrypted using AES shift rows and mix column method. The steps and algorithm is discussed below.

ENCRYPTION PROCESS

Phase-I -Rail fence transposition algorithm (Encryption process –Level 1)

Step 1: Take a text to be stored in cloud which is initially encrypted with rail fence cipher. Let the text be: SRMIST All The Best

Step 2: Consider a key (For example HACK).

Step 3: Construct a matrix of the order which is equal to the number of characters in the key considered. Here the matrix order would be 4x4

Step 4: The first row of the matrix would be filled with characters taken in the key (H,A,C and K respectively)

Step 5: Read the entries in the matrix of the order 3,1,2,4- as top to bottom reading.

Step 6: We will get the first decrypted text.

This would be the input for the second encryption process explained below.

Phase-II-Shift rows and mix column methodology (Encryption process-Level 2)

i. Calculate the number of characters (C) in the text to be encrypted. (Taken from above algorithm-step 6)

ii. Convert this text to the corresponding ASCII values.

iii. Form a matrix with these ASCII values (Ensure that the number of distinct entries in the matrix M x N >=C). Denote this matrix as P.

iv. Compute the transpose of the above matrix PT

v. We shall now get a square matrix for P T

vi. Now we consider the AES algorithm which describes Shift Row technique

The Shift-Row Transformation

Here we reallocate the bytes in every row of a matrix by a definite equalize, decided by the encryption algorithm.

The first row of the matrix is unaffected. Every byte in the second row is reallocated one place to the left. Bytes in the 3rd and 4th rows are reallocated by equivalence of two and three, correspondingly, each row n being relocated left round by n-1 bytes.

Apply this method for the matrix PT

1. Then we would construct an 8x8 key matching table. Finding out the position of the text taken (RTTeMAhsSSlBIlet) in the table . This table would fetch the (Row, Column) value number corresponding to the text given here. This step is used for key generation.
2. Construct another square matrix with the values fetched from the above step. Let this matrix be Q
3. Add this matrix Q with PT . Let the resultant matrix be R

R=PT+ Q

4. Apply the Mix column method and read the message with column mixing numbered as: 4123 .i.e Start reading in the order 4,1,2 and 3. Let the matrix obtained by this method be S.
5. Apply modulus 127 for each value of the matrix S. If the result is less than 32, add 32 to compensate for the difference between Uppercase and lowercase letters in ASCII. Let the resultant matrix be T.
6. Obtain the ASCII values for the entries in the Matrix T

Now the double encrypted data would be stored in cloud

DECRYPTION PROCESS

Phase-I -Rail fence transposition algorithm (Decryption process –Level 1)

We now give a step by step process to illustrate the double encryption process.

Rail Fence Cipher

Input Text

Encryption

Input :SRMIST All The Best

Key = HACK

Output :RTTeMAhsSSlBIlet

Take a text to be stored in cloud which is initially encrypted with rail fence cipher. Let the text be: SRMIST All The Best

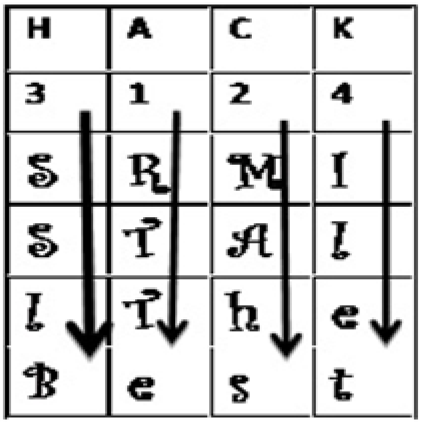
Consider a key (For example HACK).

Encryption

Input :SRMIST All The Best

Key = HACK

Output :RTTeMAhsSSlBIlet



H	A	C	K
3	1	2	4
S	R	M	I
S	T	A	l
l	T	h	e
B	e	s	t

This output/encrypted text is further encrypted using AES shift rows and mix column method. The steps and algorithm is discussed below.

Step 1: Take a text to be stored in cloud which is initially encrypted with rail fence cipher. Let the text be: SRMIST All The Best

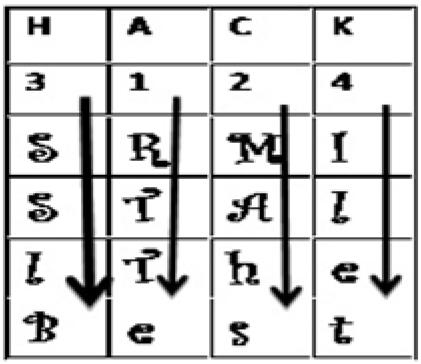
Step 2: Consider a key HACK

Step 3: Construct a matrix of the order which is equal to the number of characters in the key considered plus one row for the key value besides the number of characters in the given text (16). Here the matrix order would be 6x4 (One row for HACK, another row for the key value by which the matrix would be read and four more rows to accommodate 16 characters)

Step 4: The first row of the matrix would be filled with characters taken in the key (H,A,C and K respectively)

Step 5: Read the entries in the matrix of the order 3,1,2,4- as top to bottom reading.

Step 6: We will get the first decrypted text. This would be the input for the second encryption process explained below.



H	A	C	K
3	1	2	4
S	R	M	I
S	T	A	l
l	T	h	e
B	e	s	t

Encryption

Input :SRMIST All The Best

Key = HACK

Output :RTTeMAhsSSlBIlet

This would now be the input for AES shift row mix column encryption

Phase-II- Shift rows and mix column methodology (Decryption process-Level 2)

Step 1: Calculate the number of characters (C) in the text to be encrypted. (Taken from above step F) RTTeMAhsSSlBIlet

Step 2.Convert this text to the corresponding ASCII values.

Step 3: Form a matrix with these ASCII values (Ensure that the number of distinct entries in the matrix M x N >=C). Denote this matrix as P.

P=

82	84	84	101
77	65	104	115
83	83	108	66
73	108	101	116

Compute the transpose of the above matrix PT

PT =

82	77	83	73
84	65	83	108
84	104	108	101
101	115	66	116

We shall now get a square matrix for PT. Now we consider the AES algorithm which describes Shift Row technique

The Shift Row Transformation

This is used for altering the bytes in all row of a matrix by a value, used by the encryption algorithm.

Here the initial row of the matrix is not altered. All byte in the second row is circulated one location to the left. Bytes in the 3rd and 4th rows are disseminated by equivalence of two and three, correspondingly, each row now being circulated left circular by n-1 bytes.

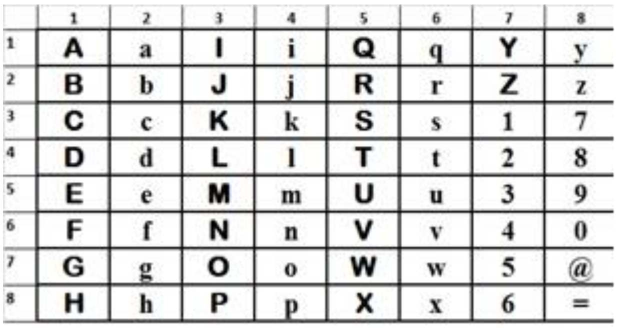
Apply this method for the matrix PT

82	77	83	73

65	83	108	84
108	101	84	104
116	101	115	66

Step 7.

Then we would construct an 8x8 key matching table. Finding out the position of the text taken RTTeMAhsSSlBIlet in the table . This table would fetch the (Row, Column) value number corresponding to the text given here. This step is used for key generation.



	1	2	3	4	5	6	7	8
1	A	a	I	i	Q	q	Y	y
2	B	b	J	j	R	r	Z	z
3	C	c	K	k	S	s	1	7
4	D	d	L	l	T	t	2	8
5	E	e	M	m	U	u	3	9
6	F	f	N	n	V	v	4	0
7	G	g	O	o	W	w	5	@
8	H	h	P	p	X	x	6	=

Step 8.

Construct another square matrix with the values fetched from the above step. Let this matrix be Q. Find the position of the text (row and column number)RTTeMAhsSSlBIleT in the above table 25,45,45,52,53,11,82,36,35,35,44,22,13,44,52,46

Q=

25	45	45	52
53	11	82	36
35	35	44	22
13	44	52	46

Step 9:Add this matrix Q with PT. Let the resultant matrix be R

25	45	45	52
53	11	82	36
35	35	44	22
13	44	52	46
82	77	83	73
84	65	83	76

84	**104**	**108**	**101**
101	**115**	**66**	**116**

R=PT + Q

82	**77**	**83**	**73**
84	**65**	**83**	**76**
84	**104**	**108**	**101**
101	**115**	**66**	**116**

+

25	**45**	**45**	**52**
53	**11**	**82**	**36**
35	**35**	**44**	**22**
13	**44**	**52**	**46**

=

107	**122**	**128**	**125**
137	**76**	**165**	**112**
119	**139**	**152**	**123**
114	**159**	**118**	**162**

Step 10:

Apply the Mix column method and read the message with column mixing numbered as: 4123 .i.e Start reading in the order 4,1,2 and 3. Let the matrix obtained by this method be S.

S=

125	**112**	**123**	**162**
107	**137**	**119**	**114**

122	**76**	**139**	**159**
128	**165**	**152**	**118**

Step 11:

Apply modulus 127 for each value of the matrix S. If the result is less than 32, add 32 to compensate for the difference between Uppercase and lowercase letters in ASCII. Let the resultant matrix be T.

T=

26	**112**	**123**	**35**
107	**10**	**119**	**114**
122	**76**	**12**	**32**
01	**38**	**25**	**118**

58	**112**	**123**	**35**
107	**42**	**119**	**114**
122	**76**	**44**	**32**
33	**38**	**57**	**118**

Step 12:

Obtain the ASCII values for the entries in the Matrix T. The result would be a encrypted text. So from the above matrix, the encrypted text would be **:p{"#*wrzL,? !&9v**

Now the double encrypted data would be stored in cloud .We now give a step by step process to illustrate the double encryption process.

STEPS FOR DECRYPTION

Step 1: Convert the encrypted text (cipher text) into ASCII values. Construct the matrix

:p{"#*wrzL,? !&9v

Step 2: Take the matrix R

107	**122**	**128**	**125**
137	**76**	**165**	**112**
119	**139**	**152**	**123**
114	**158**	**118**	**162**

Step 3: Subtract the key generation matrix from R from PT

107	122	128	125
137	76	165	112
119	139	152	123
114	158	118	162

82	77	83	73
84	65	83	108
84	104	108	101
101	115	66	116

=

25	45	45	52
53	55	82	6
35	35	44	22
13	43	52	46

Step 4: Reverse shift Row information.

Row 1 is unaltered .Row 2 is circulated left by 3, Row 3 is circulated left by 2, Row 4 is circulated left by 1

PT

82	77	83	73
65	83	108	84
108	101	84	104
116	101	115	66

therefore the reverse of shift rows would be Matrix U

82	77	83	73
84	65	83	76

84	104	108	101
101	115	66	116

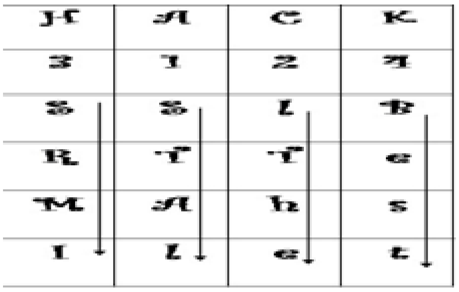
Step 5: Take the transpose of U =UT

82	84	84	101
77	65	104	115
83	83	108	66
73	108	101	116

Step 6 :Now the ASCII code values would be

RTTeMAhsSSlBIlet

Step 7: This decrypted text would again be decrypted by means of Rail Fence algorithm to obtain the original text



H	A	C	K
3	1	2	4
S	S	l	B
R	T	T	e
M	A	h	s
I	l	e	t

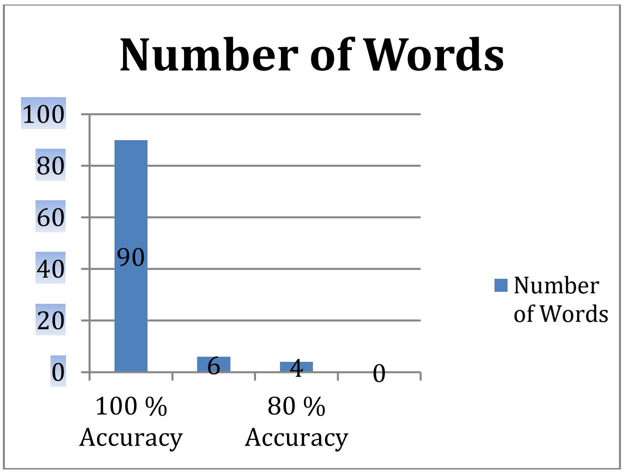
Write the text in the rail fence matrix with the order 2,3,1,4and read from the matrix
RTTeMAhsSSlBIlet
2 3 1 4
Which yields the original plain text : SRMIST All The Best

8. Results and Discussion

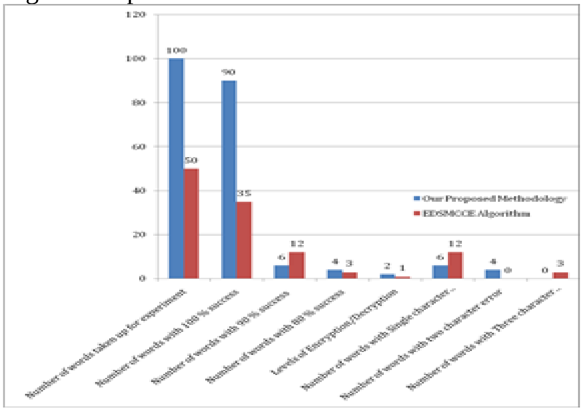
The proposed algorithm examined by using 100 sample words with different types of characters. During this study, out of 100 words90 words have been successfully encrypted and decrypted perfectly (100%). The rest of the 10 words, 6 words have contributed single character error and 4 words have resulted in two character errors. We shall measure the correctness of the algorithm with a simple equation.

Accuracy of Security = X/N *100----------(1)
X - Number of selected words
N - Total number of words

Number of words(Samples)	**ACCURACY RANGE**		
	100 %	90%	80
100	**90**	**6**	**4**



Figures: Representation of the results



Criteria	**Our Proposed Methodology**	EDSMCCE Algorithm
Number of words taken up for experiment	**100**	50
Number of words with 100 % success	**90**	35
Number of words with 90 % success	**6**	12
Number of words with 80 % success	**4**	3
Levels of Encryption/Decryption	**2**	1
Number of words with Single character error	**6**	12
Number of words with two character error	**4**	0

Number of words with Three character error	**0**	3

Table: Comparison of methodologies

9. Conclusion

Cloud computing has become a predominant technology for consumers. In the cloud storage, Security and Privacy play a major part in connection with storage and retrieval of data. Large numbers of works have been carried out in the scenario by researchers and the count still keeps on ticking every day. Different works are being done in the domain combining basic Cryptographic procedures .This paper suggested another methodology to ensure enhanced security of sensitive data in the cloud computing environment.

By smearing this double- two way encryption algorithm, the end user warrants that the sensitive data is stored only on cloud storage with increased security and it cannot be retrieved by anybody else including the administrators or invaders. Based on the investigational results, the proposed algorithm performance is good.

References

[1].SP 800-145 The NIST Definition of Cloud Computing :Date Published: September 2011 Author(s) Peter Mell (NIST), Tim Grance (NIST)

[2]. BhushanRathod, Prof. PrashantYelmar, Prof. PrachiSarode "A Survey Paper on Cloud Security Threats Issues and Attack Detection" Available from https://www.researchgate.net/publication/313222138

[3]. AnamikaChoudhary, SunitaGodara “Internet of Things: A Survey Paper on Architecture and Challenges”, International Journal of Engineering Technology Science and Research IJETSR www.ijetsr.com ISSN 2394 – 3386 Volume 4, Issue 6 June 2017

[4]. Kiruthika, U., Somasundaram, T.S. & Raja, S.K.S. Lifecycle Model of a Negotiation Agent: A Survey of Automated Negotiation Techniques. Group Decis Negot (2020). https://doi.org/10.1007/s10726-020-09704-z

[5].https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

[6].D. Sarddar, P. Sen, and M. K. Sanyal, “Central Controller Framework for Mobile Cloud Computing,” Int. J. Grid Distrib.Comput., vol. 9, no. 4, pp. 233–240, 2016

[7].R. Sumithra&Sujni Paul “ A SURVEY PAPER ON CLOUD COMPUTING SECURITY AND UTSOURCING DATA MINING IN CLOUD PLATFORM” International Journal of Knowledge Management & e-Learning Volume 3 January-June 2011

[8].RohitBhadauria and SugataSanyal “Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques”

[9].Anjali V. Almale, S.V. Phulari, ShwetsShanwad “A Survey of Data Mining in Cloud Computing” DOI 0.4010/2016.1136 ISSN 2321 3361 © 2016 IJESC

[10].Kajal Rani1, Raj Kumar Sagar2 “Enhanced Data Storage Security in Cloud Environment using Encryption, Compression and Splitting technique” 2017 2nd International Conference on Telecommunication and Networks (TEL-NET 2017)

[11].KatarzynaKapusta and Gerard Memmi A Fast Fragmentation Algorithm For Data Protection In a Multi-Cloud Environment arXiv:1804.01886v1 [cs.CR] 5 Apr 2018

[12].MaragoniMahendar, MalipatelAnusha," Privacy-Preserving Public Auditing for Secure Cloud Storage" IJ of Scientific Research in Computer Science, Engineering and Information Technology Vol. 3, Issue 1, pp.242-246, 2018.

[13].Savita.A. Harkude& Dr. G.N.KodandaRamaiah-Survey On Various Algorithms For Data Security In Cloud Computing Environment, International Journal of Computer Science Trends and Technology (IJCST) – Volume 6 Issue 6, Nov-Dec 2018

[14]Nadiah M. Almutairy, Khalil H. A. Al-Shqeerat and Husam Ahmed Al Hamad .”A Taxonomy of Virtualization Security Issues in CloudComputing Environments” Indian Journal of Science and Technology, Vol 12(3), DOI: 10.17485/ijst/2019/v12i3/139557, January 2019

[15].R.L. Rivest, A. Shamir, and L. Adleman, “AMethod for Obtaining Digital Signatures and Public-Key Cryptosystems”, Laboratory forComputer Science,Massachusetts Institute ofTechnology, Cam-bridge, November, 1977.

[16]Dr. RamalingamSugumar, K. Raja, “EDSMCCE : Enhanced Data Security Methodology for Cloud Computing Environment” International Journal of Scientific Research in Computer Science, Engineering and Information Technology,IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307,CSEIT18336 | Received : 01 March 2018 | Accepted : 10 March 2018 | March-April-2018 [(3) 3 : 40-46]

[17].RamalingamSugumar , K. Arul Marie Joycee “ADSSCCE: Analysis of Data Storage Security in Cloud Computing Environment”, International Journal of Computer Sciences and Engineering Open Access,Vol.6, Special Issue.11, Dec 2018 E-ISSN: 2347-2693

ABBREVIATIONS USED

CC	CLOUD COMPUTING
CS	Cloud Services
DoS	Denial of Service
DDoS	Distributed Denial of Service
CSA	Cloud Security Alliance
CSP	Cloud Security Provider
OS	Operating System
DC	Data centers