RESEARCH ON ADVANCES IN SECURITY OF CLOUD COMPUTING FOR DATA CONCEALMENT

Muhammad Haris Javaid, Imran Mumtaz,
Department of Computer Science, University of Agriculture Faisalabad.
Corresponding Author E-mail: harisjavaid89@yahoo.com

ABSTRACT*: Cloud computing is an Internet-based computing and next phase inside the progress connected with world-wide-web. The idea enables many users to get into the system via World-wide-web with no installation of just about any computer software. The idea store large amount of files throughout cloud safe-keeping which might be looked at by just about any part of the entire world. The idea in essence exchanges the user files in addition to program computer software to massive datacenters at the cloud, where the operations connected with files might not be completely secure. Even so, this singular attribute on the cloud computing add many security problems which should be fixed in addition to comprehended plainly. The most essential problems which should be dealt with is actually privacy in addition to security connected with files stashed throughout cloud databases. Facts security is amongst the nearly all cited difficulties which act as an impediment inside the speedy expansion connected with cloud technological innovation. Any files privacy issue appears because both system in addition to end user files are found throughout supplier areas. A lot of approaches in addition to techniques are presented to triumph over the results security difficulties although there is still need to have connected with development in this field to obtain the confidence connected with users. That investigation perform concentrates within the files privacy issue throughout cloud computing in which an superior encryption protocol is actually recommended to the concealment connected with files in this sector. We have find techniques to make data secure in cloud.*

Keywords: Cloud Computing, Data Integrity, Cryptography in cloud computing, Encryption algorithm in cloud computing, Decryption, Cloud Computing Security issues.

INTRODUCTION

Cloud computing is tremendously emerging technology, getting a remarkable attention in recent years from both academia and industry. It gives online services, cloud computing services make easy for the user to operate the online services of a variety of software instead of installing or purchasing them on their individual devices or computers.

Cloud computing is a state of mind surrounded by info imagination marketplace due to its number of factors including accessibility, little effort and better performance. This is a strategy to deal with difficulties and improve the proficiency of a link without wasting coding authorizing and fresh basic [1]. Distributed computing is an Internet-based figuring that suggested processing administrations just like programming, information, registering, stockpiling and application to nearer devices through Internet. Distributed computing is a kind of management that allows the consumer to accumulate enormous measures of information in scattered storage and use when necessary with the use of any terminal hardware from any area of the world [2]. Distributed computing is basically an Internet-based processing, that gives programming, share assets and data to personal computers and a number of devices when required [3]. information reduplication is a procedure which stores the information just once which implies that the same information can't be put away in the distributed storage zone. Information reduplication is utilized to diminish the storage room in the cloud and to effectively utilize the transfer speed for transferring and downloading the information from the distributed storage zone. Secure reduplication is a standout amongst the most complimentary and emerging test [4]. The explanation behind the theory is to ensure the security issues in the data transferring. The inside lies on how can we enhance the cloud computing security and data integrity, including the limitations and drawbacks concerning the data data being alluded to. Cloud computing has risen as a long-envisioned vision of the utility registering worldview that gives dependable and strong framework to clients to remotely store information and use on-request applications and administrations. At present, numerous people and associations relieve the weight of neighborhood information stockpiling and lessen the upkeep cost by outsourcing information to the cloud. Notwithstanding, the outsourced information is not generally reliable because of the loss of physical control and ownership over the information. Therefore, numerous researchers have focused on easing the security dangers of the outsourced information by planning the Remote Data Auditing (RDA) strategy as another idea to empower open auditability for the put away information in the cloud. The RDA is a valuable strategy to check the dependability and uprightness of information outsourced to a solitary or disseminated servers [7].

CLOUD COMPUTING CHALLENGES

Many challenges that provider and the users of the cloud computing faces are as follow.

System based distributed computing is quickly extending as another option to traditional office-based processing. As distributed computing turns out to be more across the board, the vitality utilization of the Cloud Computing is the since quite a while ago imagined vision of registering as an utility, where clients can remotely store their information into the cloud to appreciate the on-interest great applications and administrations from a common pool of configurable processing assets. By information outsourcing, clients can be alleviated from the weight of neighborhood information stockpiling and upkeep.the way that clients no more have physical ownership of the conceivably extensive size of outsourced information makes the information trustworthiness assurance in Cloud Computing an exceptionally difficult and possibly impressive errand, particularly for clients with obliged registering assets and

abilities. Along these lines, empowering open auditability for cloud information stockpiling security is of basic significance with the goal that clients can turn to an outer review gathering to check the trustworthiness of outsourced information when required. Cloud computing gives assets and shared administrations through the web. Administrations will be conveyed through the server farm. Distributed computing gives a fascinating business proposition to data innovation industry, which with no extra speculation, clients can do overwhelming preparing by gadgets, for example, a cell phone that has the assets including the web program to run. Then again, distributed computing has been liable to numerous security issues. At the point when a customer conveys his information to a cloud supplier for sparing, there is the likelihood of information misfortune. From the point of view of clients, distributed computing security concerns are still set up, specifically issues identified with information security and protection assurance. In this paper, the difficulties and security issues in distributed computing are explored from two points of view being information security and protection insurance [8].

To secure the information in cloud database server cryptography is one of the critical strategies. Cryptography gives different symmetric and hilter kilter calculations to secure the information. This paper displays the symmetric cryptographic calculation named as AES (Advanced Encryption Standard). It depends on a few substitutions, stage and change. Watchwords [9]. It is an adaptable, financially savvy, and demonstrated conveyance stage for giving business or buyer IT benefits over the Internet. In any case, distributed computing presents an additional level of hazard since basic administrations are regularly outsourced to an outsider [10].

In Numerous organizations, for example, Amazon, Google, Microsoft etc, quicken their paces in creating Cloud Computing frameworks and improving their administrations to accommodate a bigger measure of clients. In any case, security and protection issues show a solid boundary for clients to adjust into Cloud Computing frameworks. In this paper, we explore a few Cloud Computing framework suppliers about their worries on security and protection issues. adjusting discharged represents new situations in the Cloud, it will bring about more clients to venture into Cloud. We assert that the success in Cloud Computing writing is to come after those security and protection issues having be determined.

Customers try not to have control above the servers of cloud temporary workers. They need to select an organization for facilitating or administration contractor that has versatile and steady cloud server structure. Considered power outage issue is completely required to settle on a decision about selecting the organization supplier. In addition, simplicity of comprehension of Internet affiliation will settle on access to your framework. Structures can go down at whatever point is a key that should recall if one's are thinking about exchanging to the cloud.

Safety of customer’s material is he most raised up issues now distributed mechanism. Material confidence may stay a remarkable kindness to consumers who wants to provide distributed mechanism. Distributed computing improvement desires justifiable endeavors to build up arrangements to clear customers' mindfulness toward representation, most cloud customers have stresses over their private data that it may be switch to other cloud organization providers. The consumer information should be protected incorporate four divisions including:

Information utilization; data collected from personal computers gadgets

Sensitive information; information on money related equalization, prosperity record et cetera

Data that can remain used on behalf of distinguishing verification of specific

Security is a key concern when embracing cloud innovation. Cloud arrangements incorporate not just issues acquired from related innovations, for example, virtualization and disseminated processing, additionally new concerns related to many-sided quality of the cloud environment, formed by the cloud elements and their cooperations. One of the worries is identified with validation and approval in the cloud so as to give powerful systems to recognize elements and set up their consents and parts in the cloud, controlling asset utilization and advancing bookkeeping and detachment. This paper distinguishes the best in class as far as certification administration concentrating on the cloud environment.

CLOUD COMPUTING SECURITY ISSUES

Respectability Distributed computing has been imagined as the cutting edge engineering of IT Enterprise. It moves the application programming and databases to the unified huge server farms, where the administration of the information and administrations may not be completely dependable. This interesting worldview realizes numerous new security challenges, which have not been surely knew. This work examines the issue of guaranteeing the trustworthiness of information stockpiling in Cloud Computing. Specifically, we consider the undertaking of permitting an outsider evaluator (TPA), in the interest of the cloud customer, to check the honesty of the dynamic information put away in the cloud. The presentation of TPA dispenses with the contribution of customer through the reviewing of whether his information put away in the cloud is without a doubt in place, which can be imperative in accomplishing economies of scale for Cloud Computing.

In Software as a service irregular information is gained from attempts and set away at the SaaS business end thereafter took care of by SaaS application. A need to secure all data streams over the framework keeping in mind the end goal to stay away from surge of discerning data. These include the utilization of solid system movement encryption strategies just like Secure Socket Layer (SSL) for security and Transport Layer Security (TLS).

In the event of Amazon Web Services (AWS), the system provides huge assurance against conventional system security issues, e.g., port checking, bundle sniff, Internet Protocol satirizing and onwards. Mush elevated assurance, Amazon S3 is accessible by means of SSL programmed nodes. They scrambled end centers that are nearby together from the Internet & from esoteric Amazon EC2. Be that as it may, unapproved clients can take the upside of feeble center of

attention in system setup protection by sniffing system bundles.

MATERIALS AND METHODS

It disposes of the need to keep up costly processing equipment, committed space, and programming. Huge development in the size of information or enormous information produced through distributed computing has been watched. Tending to huge information is a testing and time-requesting errand that requires a vast computational foundation to guarantee fruitful information preparing and examination. The relationship between enormous information and distributed computing, huge information stockpiling frameworks, and Hadoop innovation are additionally talked about. Moreover, explore difficulties are researched, with concentrate on versatility, accessibility, information trustworthiness, information change, information quality, information heterogeneity, protection, legitimate and administrative issues, and administration [5]. Offering continuous information security for petabytes of information is essential for distributed computing. A late review on cloud security expresses that the security of clients' information has the most astounding need and additionally concern. We trust this must have the capacity to accomplish with an approach that is efficient, adoptable and very much organized. Along these lines, this paper has built up a system known as Cloud Computing Adoption Framework (CCAF) which has been tweaked for securing cloud information. This paper clarifies the review, method of reasoning and segments in the CCAF to ensure information security. CCAF is represented by the framework configuration in view of the prerequisites and the execution showed by the CCAF multi-layered security. Since our Data Center has 10 petabytes of information, there is an immense errand to give continuous assurance and isolate. We utilize Business Process Modeling Notation (BPMN) to reenact how information is being used [6].

For testing the security of data of cloud computing a scenario based study has been held by using both techniques (old vigenere & e-vigenere). For this research, examples are used which are first crypted & decrypted by a keyword using old method and then using proposed method. After that both results will be matched. based) have been run; their performance is measured and compared. Examination of cloud security is measured by making different scenarios with and without security measures and both results are compared. As we know that cryptography has two kinds:

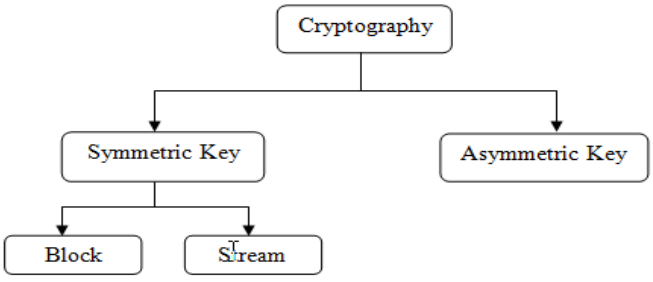

Fig.1 Cryptography

Fig.1 is explaining the types of cryptography. As we use symmetric key so it us further shown in it`s types. Our proposed method underpins poly-alphabetic replacement technique by which figure character got by fix expansion of simple content & key character and every figure character will be replaceable with few dissimilar characters. Following are the tables for the numeric estimates of letter set.

Table 1

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Table 2

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Table 3

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Table 4

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Table 5

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Table 6

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Table 7

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

Table 8

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

Fig.2 Table

Technique for key generation

In our suggested method three steps are involved. Firstly, key will be generated between the user who will upload the file and the service supplier both are cloud based. Then it will be encode & decode at the same time because our algo is symmetric.

After the key generation file will be encrypted and stored in cloud data center. Following is the enhanced vig algorithm:

Enhanced Algorithm

1. Plain Text
2. While (text is not end)
   - 2.1 num ← 1
   - 2.2 From plain text read the next character
   - 2.3 Matching the plain text + character key from Table=num
   - 2.4 Generation of cipher text keyword S= (simple text char + keyword) % 26
   - 2.5 num++
   - 2.6 if (num>8)
   - 2.7 num=1

In our proposed technique 1st alphabet of plain text and key will be encrypted by using table 1 and 2nd alphabet of plain text and key will be encrypted by using table 2 and so on.

This will go up to 8th table i.e.8th alphabet of plain text and key will be encrypted by using table 8. Then 9th alphabet of plain text and key will be encrypted by using table 1 and so on. The formula for encryption is:

Si = Li + Qi (mod m) from table 1 to 8

Where,

S = Cipher character

L = Plain text character

Q = Key phrase character (If the key size is small than the size of plain text, then key will be continue until it becomes equal to the length of simple text).

n = alphabets length

We can additional simplify the formulation as:

$S1 = L_1 + Q_1 \pmod{26}$ from table 1, where A=0, B=1, C= 2 .... Z=25

$C_2 = L_2 + Q_2 \pmod{26}$ from table 2, where B=0, S=1, D=2..... Z= 24, A=25

$S_3 = L_3 + Q_3 \pmod{26}$ from table 3, where S=0, D=1, E=2..... Z=23, A=24, B=25

.

.

.

$S_8 = L_8 + Q_8 \pmod{26}$ from table 8, where H=0, I=1, J=2..... G=25

$S_9 = L_9 + Q_9 \pmod{26}$ from table 1

$S1_0 = L_{10} + Q_{10} \pmod{26}$ from table 2

.

.

Si = Li + Qi (mod m) from table 1 to 8.

Decoding is the converse procedure of encryption it works in same route as encryption yet in opposite.

RESULT AND DISCUSSION

Now we take some different examples and will solve it by using old & our proposed technique and them compare the both results to identify the security, performance and time complexity strength, First let us see how old method works. An old-style vigenere square table given under:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig.3 old vigenere table

Fig 3 showing the old vigenere table for mapping. Let us encode n-th word of the exposed content by-using the Vigenere square method, firstly we calculate the x-axis (e.g. "H") in vignere-square table, now we catch word of given key phrase (e.g. "F") lies y-axis. Then crossing point of given row & column is our n-th word of cipher text (M). Similarly for decoding the cipher word, we find rows matching with n-th word key ("F") the chamber in which the n-th word of cipher text ("M") exist in. Their column is given by n-th word of open text ("H").

We study the below table for encoding & decoding.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fig.4 Table

Fig.4 showing the enhanced form of table for mapping.

Si = Li + Qi |mod of m |

Li = Si- Qi | mod of m |

So,

Si = c^{th} letter of the encoded text

Li = r^{th} letter of the plain text

Qi = c^{th} letter of the encoded-key (simple text will be generated if key is small, we repeated until it becomes equal to the simple text size).

n = length of the alphabet

e.g. , given simple text is "E" & key letter is "I" and size of letter is 26 then;

$B_D = E + I = 4+8 \mid 26 \mid = 12 = M$

$L_k = M - I = 12-8 \mid 26 \mid = 4 = E$

Encryption of a single word by using a single keyword

Now we will convert a text in to a cipher-text with a key by using both vigenere and suggested e-vig techniques.

Key-phrase: FSD

simple-text: HELLO

Plain Text	Key	Cipher text
H	F	M
E	S	W
L	D	O
L	F	Q
O	S	G
H	D	K
E	F	J
L	S	D
L	D	O
O	F	T
H	S	Z
E	D	H
L	F	Q
L	S	D
O	D	R
H	F	M
E	S	W
L	D	O
L	F	Q
O	S	G

Fig.5 Encryption with Vigenere algorithm

Now we encode the above case by E-Vig algo.

Plain Text	Key	Cipher text
H	F	M
E	S	V
L	D	M
L	F	N
O	S	C
H	D	G
E	F	D
L	S	W
L	D	O
O	F	S
H	S	X
E	D	E
L	F	M
L	S	Y
O	D	L
H	F	F
E	S	W
L	D	N
L	F	O
O	S	D

Fig.5 Encryption with E-Vig algorithm

Now by comparing the two results of encryption & decryption by using two different methods i.e. Vigenese & e-vig, we can clearly see the cipher text is repeated and it makes cool for attackers to figure out original size of key by using "kasiski attack" or by performing brute-force will get the original text. On the other hand , when we applied e-vig algo it doesn't repeat the cipher text and this makes it strong against kasiski & brute- force attacks. It will be very difficult for the attackers to find the original text.

Encryption of big data

Now let's examine the following text, we will first encode it using Vigenere encryption method and then using e-vig encoding method to compare the outputs of both methods. "FAISALABAD" is the text which is used to encode the key-phrase.

Plain text (242 characters)

UNIVERSITY OF AGRICULTYRE FAISALABAD HAS EMBARKED ON A NEW PHASE OF HISTORY GOVERNMENT COLLEGE UNIVERSITY HAS A LONG HISTORY OF EXCELLENCE AND DISTINCTION AS AN INSTITUTION IT IS BUSY IN THE PREPARATION OF A DEVELOPMENT PLAN BOTH IN TERMS OF EDUCATION AS WELL AS PHYSICAL DEVELOPMENT.

Ciphertext with traditional Vigenere encryption technique

LODWRYMFNW HOTDERE VNLAEZKIEY GALXATSBLD IAV JMJSRVEE OQ F NMO PSATE RK HQKTZRZ GRAEZFMPNU CRQLMYE FNJVHWSQLY SAT A OTNO ZIDTPRB TF MPCPLMEQHE IFD OITTLSCBAOY AT AQ NNALIEUUIRS IB AS MUTY LS TPW PCEQAUFTQGN ZF B DHAETGPXEOT SQAV TOEH JN WJRUK OQ EEUFFTQGN LS XEOQ AA HHJSJCDQ DMNEWOQMHST

Ciphertext with proposed EVig encryption technique

LNBTNTGYNV FLPYYKE ULIWZTDICW DWGRTTRZIZ DUO JLHPNQYX OP D KIJ JLASC OG CKDTYPW CMUXZEKMJP WKQKKVA AHCVGUPMGS LAS Y LPII SICRMNW NY MOAMHHWJHD GCZ JCMTKQZXVIR AS YN JIUEIDSREIM BB ZQ JQOS ES SNT LXYJATDQMBH SF A BEWZNZPWCLP NKTV SMBD EH PJQSH KL YXUEDQMBH ES WCLM VU AHIQGYYK WMMCTLLGASS

In the above encrypted methods every cipher text characters denotes 26 unlike arrangements and it will give 676 total combinations. On the other side in old Vigenere method every arrangement gives precisely 1 cipher character each interval. So, it is cool for attackers towards guessing the scheme of cipher-character & supposes there is uncertainty that attackers get ahead in discovering the encoded key then it is much cool to get the text. On the other side, using our given e-vig encryption method can gives eight unique cipher characters from every combination.

Some important facts- finding of above case are given below in tables: -

Plain Text Character No.	Combination of plain text and Key character	Vigenere Technique result	Proposed EVig technique result
2	O & A	O	N
12	O & A	O	L
49	O & A	O	O
135	O & A	O	I
195	O & A	O	M
205	O & A	O	K
237	O & A	O	L
19	N & A	N	L
52	N & A	N	K
77	N & A	N	J
87	N & A	N	H
102	N & A	N	I
39	A & A	A	U
99	A & A	A	Y
169	A & A	A	A
192	A & A	A	T
222	A & A	A	V
60	O & D	R	O
70	O & D	R	M
80	O & D	R	K
150	O & D	R	I
134	I & S	A	V
143	I & S	A	U
154	I & S	A	Z

Fig 6. Comparison Table

Frequencies of cipher characters by using vigenere - e-vig methods are shown in above table. Now, we notice that by using vigenere method character is repeated when the combination is repeated e.g. when O&A occur it always gives character "O", O&A is repeated 7 times and 7 times the resultant character is "O". While in e-vig method when O&A occur the result is a different character always As O^D repeated 4 times so old algo gives 4 times "R" cipher-text.

While examining the suggested e-vig method outputs are different than vigenere method. For example, the set O&A is repeated 7 times but it gives 7 unique characters i.e. (N.L.O.I.M.K.I) and O&D is repeated 4 times and the result is (O.M.K.I) in Traffic received at mobile nodes at the begging is very high then it is decreased and the less traffic is

received in all the three scenarios. Means the web performance is almost same in all three scenarios.

Recurrence study of basic text, old vig cipher & suggested e-vig cipher as of the text from scenario 2 is under below table. The table reflects that frequency test of suggested procedure is much challenging as associated to traditional method.

CONCLUSION

After studying this we came to the result that our suggested method is much efficient and stronger than the old version of vigenere algo to analyze the performance and efficiency wo examine two cases and perform both methods on it one by one. From both two cases we came to see that in vinegere algo method when the same combination happen the resultant cipher text is same, while by performing e-vig algo method if the arrangements repeated then a unique cipher-text generated every time. There is no repetition. Because of this method it becomes difficult for brute-force attack, cryptanalysis & pattern prediction. We also perform performance analysis to check the efficiency of our suggested method and it shows that it is nearly like the old vigenere-cipher. So, we can say that our suggested method removes the flaws of old vigenere method and is much stronger for data privacy then vigenere method.

REFERENCES

[1] Soofi, A. A., and M. I. Khan. A Review on Data Security in Cloud Computing. *International Journal of Computer Applications*, 94(5):12-20 (2014).

[2] ChingNung, Y., and I. Jia-Bin. Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing. *Biometrics and Security Technologies (ISBAST)*,12:25-29 (2013).

[3[Mishra, N. A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues. *International Journal of Science, Engineering and Technology*. 2(1):59-68 (2015).

[5] Hashem, I. A. T., I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan. The rise of big data on cloud computing. *Review and open research issues. Information Systems.* 47: 98-115 (2015).

[6] Chang, V., and M. Ramachandran. Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing*. 9(1):138-151 (2016).

[7] Sookhak, M., A. Gani, H. Talebian, A. Akhunzada, S. U. Khan, R. Buyya, and A. Y. Zomaya. Remote data auditing in cloud computing environments. *A survey, taxonomy, and open issues. ACM Computing Surveys (CSUR).* 47(4), 65 (2015).

[8] Shariati, S. M., and M. H. Ahmad zadegan. Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection. *2nd IEEE International Conference on Knowledge Based Engineering and Innovation (KBEI)*.1078-1082 (2015).

[9] Pancholi, V. R., and B. P. Patel. Enhancement of Cloud Computing Security with Secure Data Storage using AES. *International Journal for Innovative Research in Science and Technology*. 2(9):18-21 (2016).

[10] Hashizume, K., D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*. 4(1), 1 (2013).