International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

# Enhancing Security in Cloud Computing using Playfair and Ceasar Cipher in Substitution Techniques

**S.Karthiga, T.Velmurugan**

***Abstract:*** ***Cloud Computing is playing the significant role in the existent submissions the humans life. Cloud computing is an extravagant set of conveniently and operative virtualized assets, like as hardware, evolution platforms and utility. Cloud computing is a exclusive generation of the parallel conception. The cloud computing extensibility is a concern of the allotment of revenue on mastery demand. Cloud computing accommodate the operation of uniting. The elevation of the cloud automation also raises the security controversy twice. So, there is a need to solve the security contention in the cloud automation. Reasons for maturity of cloud security for disparate inhabitants and disparate prospect depend upon the exaction. The main trouble correlate with cloud computing is data confidentiality, preservation, data stealing, data breaches etc. In this research work, it is proposed to use a new level of data security solution using Playfair cipher and Ceasar cipher algorithm. Both the algorithms are encrypted by the full set of 256 ASCII characters. A new encryption algorithm for security is implemented in this work. The main aim of this research work is to clarify the security issues in both cloud providers and cloud consumers using cryptography encryption methods.***

***Index Terms— Cloud computing, Cloud Security, Playfair Cipher, Ceasar Cipher, Network Security.***

## I. INTRODUCTION

Cloud computing is a emphasis that pore on intimacy collection and procedure over a ascendible network of nodes, extending across end user computers, data centres, and web services. Nodes from ascendible network form a cloud. Machinery which is rudiments on these clouds is advised as cloud utilization. The cloud Security confluence of real inflection change in which way the systems are positioned is executed by the cloud computing and to inception the cloud computing is very small and with this it can become big and very fast. M. Armbrust et al., discussed in the research article[1]. In the survey paper Mobile cloud computing: A survey, Future Generation Computer Systems proposed by N. Fernando et al., about Cloud Computing is the key agenda in slight, medium and huge assess convention and as many cloud end users dig for efficacy of cloud computing, the beyond engrossment is the resistance of intelligences in the cloud.

**Revised Manuscript Received on February 28, 2020.**
***** Correspondence Author
**S. Karthiga***, Research Scholar, PG and Research Department of Computer Science, D G Vaisnav College, Chennai, Tamilnadu, India.
**Dr. T. Velmurugan**, Associate Professor, PG and Research Department of Computer Science, D G Vaisnav College, Chennai, Tamilnadu, India.



Attaining data is always necessary relevance followed by humbling texture of cloud computing and the extensive amounts of assorted data it convey, the need is even more significant [2]. B. Hayes explicate about the prospective cloud users and its isolation in the research article. Hence forth, involvement about data privacy and security are examining to be an enclosure to uptake of cloud computing services.

Every cloud service(s) suitor a specific or a league should demand the right investigate to the cloud provider before receives their reports or applications on the cloud. Are they pecuniary vibrant? Do they have good security scheme and customs in place? Is the underpinning meant to host your report shared with lots of surplus users, or will it be segregated by virtualization? As many companies move their files to the cloud data undergoes much revolution and there are many claiming to conquer. To be effective, cloud data security build up on more than ease to apply data security procedures and counter measures[3].

The research paper is organized as follows. Section 2 provides related work through literature survey. Section 3 demonstrates material and methods of this research. Experimental work with a discussion is given in section 4. Finally, the conclusion of this work is pointed out in section 5.

## II. LITERATURE SURVEY

A number of researchers have done their research in the field of cloud security. Few of such type of articles are discussed in this section. H. T. Dinh et al., described about the architecture view in the survey paper, It is a tolerant of diffuse computing where aggregate flexible IT-dependent potential are render to varied surface users using web application. The service providers have to resolve a large computation technologies; and virtualization of structure for assorted users and services providers to provide the multiple utilization services examined in the survey paper [4].

Figure 2.1 explained how the cloud is adopted all over the systems. Cloud services can be accessed and used in all systems. The software is enhanced more acquire and yielding for the customer benefit and it afford a low-cost origin point in hardware enlargement, with a smooth and cost-effective promote artery to scale as service grows, designed by Y. Jadeja et al., [5]. M. A. Vouk described about cloud computing user and providers in its research paper. The platform of storage provides tons of utilization for enjoyers.

Therefore change the authority of CC and frame individual. Effort to salvage the appropriate resources in the summarized allotment is an important topic. In CC ambiance, customer can approach the operable adequacy hurried with net usage, and the systems have the huge assurance to crank the utility inquiry from frequent enjoyer in the ambiance [6].

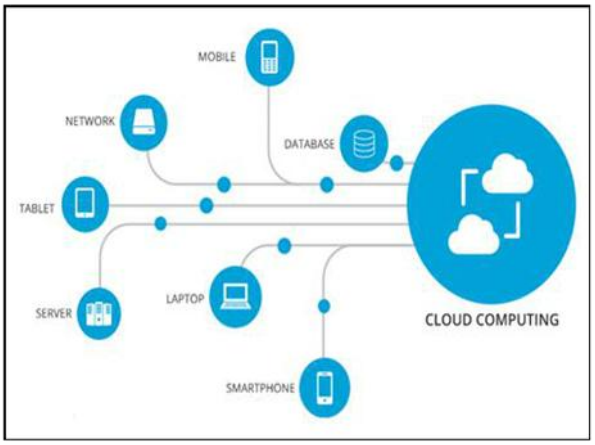


**Figure 2.1: Cloud Architecture**

Cloud computing - Issues, analysis and performance exploration paper discusses about the internet users and cloud embrace by the conformation. The internet underpinning is consecutive enlargement occurrence that frequent relevance assistance can be accommodating in the net. In a diffused computing system, element set aside to diverse places or in separated entity are applicable so that they may combined be used to higher protection [6]. Furthermore, much application of cloud computing can increase user convenience.

### 2.1 Security Challenges in Cloud Computing

The cloud relevance providers make assured that the user didn't visage all Commotion like as predication of report or data theft. There are 5 types of contention derive while contend salvation of a cloud in data breach.

**Data Issues:** Dispatching CC redemption contention narrates about the data controversy in the cloud framework. Data piracy is a special of grim contention in a CC ambiance. Data perdition is a typical complication in cloud computing. In addition, data perhaps disoriented or deprivation or perverted in behalf of miss proceeding, consistent misfortune, and embers. Data assurance in cloud computing is especial significant cause it could be involved for the cloud user to adeptly review the observance of the cloud supplier and as a determination self-sufficient that circumstances is managed. Also very expert report in corruption custom in cloud computing proposed by D. Zissis and D. Lekkas [7].

**Privacy Issues:** I. A. T. Hashem discussed and highlighted the solitude contention in the cloud computing service provider must make sure that the customer claimed orientation is robust acquire from other provider and user. Authentication is a terrific explication for the concealment controversy in the research work.[8].

**Infected Application:** A view of cloud computing research article elucidate about influence employment and its qualified enjoyer from uploading any influence relevance onto the cloud which will individually induce the customer and to baffle cloud service provider should have the exhaustive avenue to the server with all rights for the animus of observe and conservation of server proposed by M. Armbrust *et al* [9].

**Security issues:** M. Ali et al., published the immunity issues in the research paper, CC refuge to be done in two levels. The enjoyer should determine that there should not loss of data or stealing or tampering of data from other customers that who are using the same cloud due to its process. Cloud service provider makes sure that the server is well secured from all the external threats it may come across in the research paper security in cloud computing: opportunities and challenges [10].

**Trust Issues:** The survey paper confect about devoted regularity written by D. Sun et al., Trust is very necessary appearance in vocation. Still cloud is decline to make expectation amidst customer and provider [11]. The data breach guarantee is the confront one in cloud server. The stability of data loss and data breach is highly convened in the research paper. The figure 2.2 highlighted some security challenges in the cloud server.

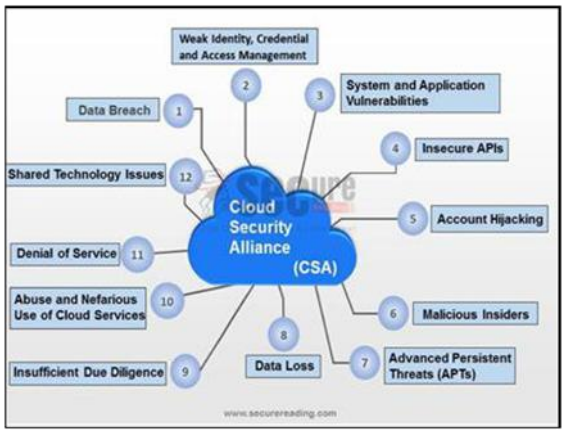


**Figure 2.2: Cloud security challenges**

## III. MATERIAL AND METHODS

CC is a gamp phrase used to attribute to Internet based development and services. A cloud client subsists of computer hardware and/or computer software that relies on cloud computing for application delivery in the research paper [12].

### 3.1 Description of Dataset

Preservation contrivance for CC and data pledge entity to appliance into the cloud computing using Playfair and Ceaser cipher in Substitution Techniques and the earnest architecture of augmenting security in Cloud Computing using Playfair and Ceasar cipher in Substitution Techniques the system is devised by using encryption and decryption algorithms which eradicate the hustle that occurs today with snatched in the cloud computing atmosphere and the security data written by A. Bhardwaj et al., [13]. The algorithm steps are follows.

1. Receive the clear text.
2. Receive the Identification.
3. Modify the Characters into binary form.
4. Apply the Formula to bring the encrypted and decrypted message.

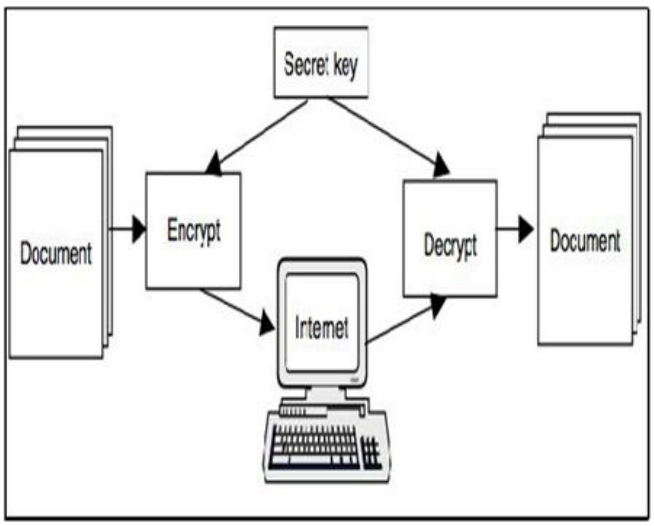


**Figure 3.1: Substitution technique**

E. Hairer written in the research paper about the security algorithms in differential forms, the main contribution of this paper is the new view of data security solution with encryption, which is the important and can be used as reference for designing the complete security solution in its research paper [14]. Figure 3.1 described substitution technique and how the data are guard in the cloud server. Top Pressures in 2016 the book recognized about altered varieties of threats in the cloud structure, the circumvention algorithms using substitution technique is discussed in the book. The Cloud security is very important for Cloud service providers and Cloud users. Both the user is high inadequate of preserve. Cloud user who loss data are facing depletion of security issues. There is a one best solution is providing a high security for cloud users is password protections are written in the book [15]. D. Chen and H. Zhao discussed about confidentiality retreat of cloud computing, the actual cloud service provider's gives 144 characters password and it transformed into ASCII code and store in the servers. The password is cracked by hackers easily and crashes the cloud user's files. In this research paper we introduce 254 character passwords and it converted into corresponding ASCII code to preserve the cloud data. It provide further immunity for cloud service providers and cloud users[16].

### 3.2 Playfair Cipher and Dataset

S. Basu and U. Kumar Ray written in the research paper about playfair algorithms in the named research article "Modified Playfair Cipher using Rectangular Matrix". Playfair is hence forwarded utilized by military coercion due to the feature of digital encryption

appliance. Such cipher is present curiosity to the Playfair cipher uses comforts contain a vital word or phrase. Recognition of the code word and cause was all that imperative to contrive the console and utilize the cipher[17].

Rahim, R., & Ikhwan, A discussed in the research article ventilate about key formation. To induce the key wagon, precise effect in beginning filter the spaces in the console with the alphabets of the access, then filter the salvage spaces with the ease of the alphabets of the alphabet inadequate. The primary could be drafted on lead succession console in anti-clockwise template or in different format, like as coil pattern in the upper-left-hand intersection followed by closure on the centre. There will not be any impact in the assembly for layer in console on the cipher [18].

To encode a dispatch, we have to divide the note into figure. For ex: "Hello World" changes to "HELLO WORLD". These diagrams will be replaced using the key console. Has encryption desire usage sign, dispatches with a random number of characters usually appended an extreme letter, like as "X", to extensive the ultimate diagram. The two letters of the diagram are examined opposite vertices of a plane in the basic console A. Lecturer and D. A. Hammood written in the research paper Breaking A Playfair Cipher Using Memetic Algorithm [19]. Murali et al., discussed in its research paper about stride to variations of algorithms, to apply the following 4 rules in figure 3.2 regularity, to each combination letters in the clear text register. There are several slight modification of the primitive algorithms in Playfair cipher [20]. Figure 3.2 explain the playfair encryption algorithm and bumpy forecast are contest in the diagram.

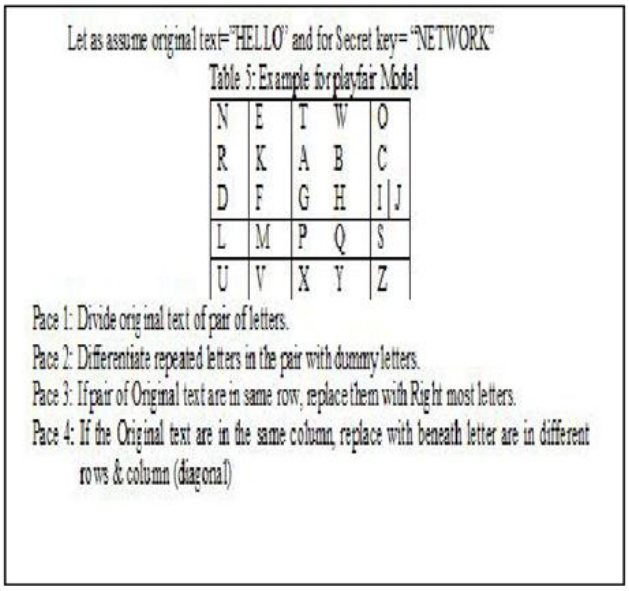


**Figure 3.2: Playfair cipher encryption**

To decode, use the flip of the last 3 guideline (reducing any further node that do not make impact in the closing intimation when finished).The decryption of playfair cipher is given in the figure 3.3.

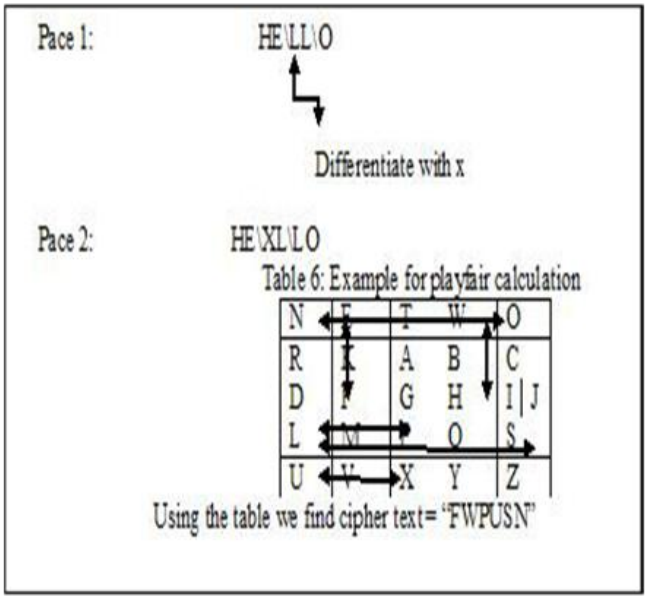


**Figure 3.3: Playfair Decryption**

### 3.3 Ceaser cipher and Data set

The Caesar Cipher performance is one of the primitive and smooth methods of encryption approach. It directed a variety of substitution cipher, i.e., each character of a given text is regained by a letter some attached count of tracts inferior the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The process is apparently named behind Julius Caesar, who probably used it to interact with his officials, J. F. Al-Muhtadi, et al., discussed in its research article [21]. In the research paper An Improved Cryptographic Technique to Encrypt Text using Double Encryption discussed about dataset and algorithms of ceaser cipher. Thus to cipher an obsessed content need an integer value, known as shift which demonstrate the number of position in the word to each letter of the text has been moved down. The formula for ceaser cipher is important to secure the files and it is helpful to shield the information and passwords in the cloud. The encryption can be defined using modular arithmetic by first convert the letters into numbers, admit to the scheme, X = 0, X = 1, N = 25 [22]. Encryption of a letter by a shift n is calculated by using formula (1).

$$E_n(x) = (x + n) \bmod 26 \quad (1)$$

The decryption letter by a shift n is calculated by using formula (2).

$$Dn(x) = (x - n) \bmod 26 \quad (2)$$

Y.Rajput proposed the Ceaser cipher formulas are used to encrypt and decrypt the data. Ceaser cipher is used to protect the cloud data as well as provide more security for cloud users and cloud provider from hackers. The files will be secured using password protections. The passwords are encrypted using Ceaser cipher algorithms in its research paper [22]. The example for ceaser cipher encryption procedure is given in the figure 3.4.

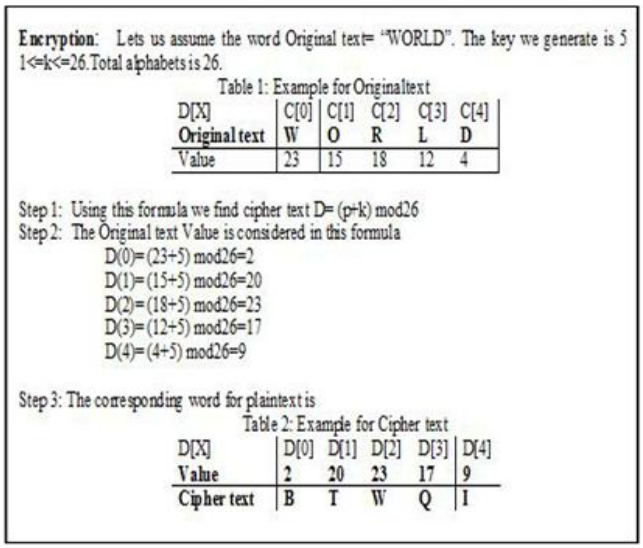


**Figure 3.4: Ceaser cipher encryption algorithm**

J. F. Al-Muhtadi et al., discussed about the decryption of ceaser cipher is little bit differ to compare of encryption algorithms. The same secret key will be used in the decryption algorithms and the ceaser cipher formula will be used in this example in the research [21]. The decryption is given in the figure 3.5.

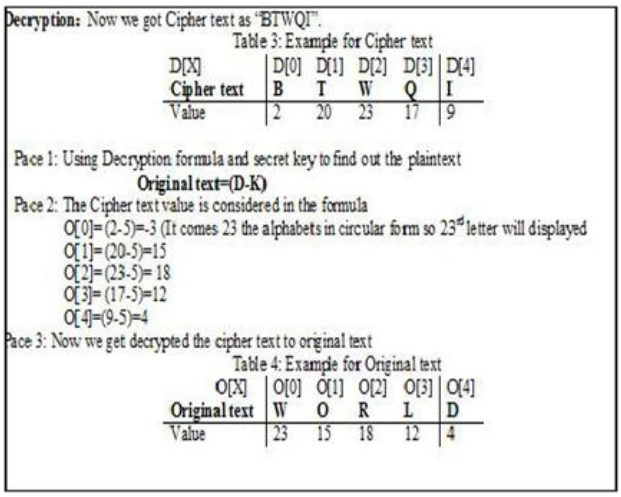


**Figure 3.5: Ceaser cipher Decryption algorithm**

In the research paper data security and privacy in cloud computing discussed about data breaches and its useful. The imperative of shade against enlarging hazard to the cloud is a humbling concern in this year. Fortunately, there is yielding, well-tested explication unfolding [23].

## IV. EXPERIMENTAL RESULT

A Cloud environment is dependent to comparable menace as acknowledged communal hook-up as well as new access of attacks by the way of mutual effects, cloud service providers gives contract to third diversion helpmate to the cloud prospect. The exposure of data breaches is not exclusive to cloud computing, but it typically ranks as a concern for cloud prospect.

Berl, A et al., dissert about the data breaches and the refuge needs in the research paper Energy-efficient cloud computing, organizing encryption software in the cloud can moderate the opportunity of data breach in the action of an attack.

Cloud encryption can added blunt the encounter to a agenda mutual model and distinction when a breach does arise in the cloud server [24]. Figure 4.1 describe the adoption of substitution technique in the cloud environments.

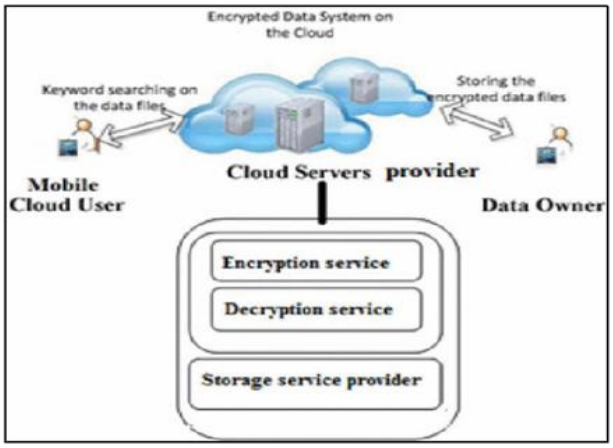


**Figure 4.1 Cloud server using Substitution technique**

**Results of Playfair cipher**

In Cloud computing the substitution technique is providing additional security for cloud users. The cloud users are facing lack of security for their files. The cloud infrastructure is weak entity so easily the data will be lost and hacked the user account and the organization secured data will be leaked and data breach is hacked easily.

In the research paper described about providing additional security for cloud users and cloud providers. The Encryption and decryption algorithms are provided to secure the data breach to avoid stolen data. The figure has shown the result of playfair cipher to encrypt the password in the cloud server. The Secret key is given for users by service providers. The secret key is lost or forgotten means the data will be locked by service providers. Figure 4.2 is shown the result of substitution technique in the cloud architecture.

```
Enter key: NETWORK
Enter the plain text: I LOVE INDIA
N E T W O
R K A B C
D F G H I
L M P Q S
U V X  Z
Entered text: I LOVE INDIA
Cipher Text: HZSNEKZHRLGC
```

**Figure 4.2: Playfair cipher using characters**

Data security demanding and its clarification in cloud computing research article confer around the cloud bond and its petty purist and worthless regularly predicate are resistant to data breaches. Compressive frameworks conduce to unduly intrepid that they are disguised against this exposure. Horribly, the number of latitude towards data breaches is enlarging every year, and no outfit or production is secure. In there were 791 data breaches rumoured a 29 holdout accumulation related to the equivalent measure in 2016. The data loss in crush frameworks in manufactory proposed by R. Velumadhava Rao and K. Selvamani [25].

```
Enter key: COMPUTER
Enter the plain text:Dragonball@123
C O M P U
T E R A B
D F G H I
K L N Q S
V W X  Z
Entered text: DRAGONBALL@123
Cipher Text: GTRHMLTBNWNWNWNW
```

**Figure 4.3: Playfair cipher using numbers**

In playfair cipher the all ASCII characters is accepted, in this example the plain text given in combination of numbers and characters and the result came in characters. The result is shown in figure 4.3.

```
Enter key: India
Enter the plain text: sharma34%91
I N D I A
B C E F G
H K L M O
P Q R S T
U V W X
Entered text: SHARMA34%91
Cipher Text: PMDTOIOIOISI
```

**Figure 4.4: Playfair Cipher using special characters**

In the figure 4.4 shown the plain text contains characters, numbers and special characters. In this example the plaintext accepts all ASCII characters and made decryption according to the plaintext characters. Some ASCII characters not accepted in the playfair cipher.

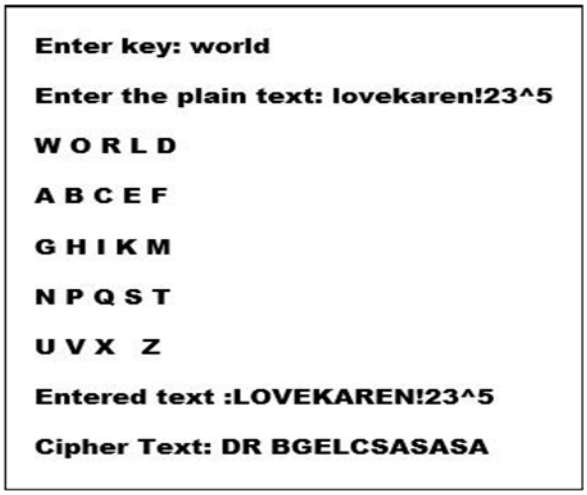


**Figure 4.5: Result of playfair cipher**

In figure 4.5 the result shown the playfair cipher accepts alphabets, numbers, and special characters. The plaintext will accept 144 bits of data. And decryption made according to the plain transcript. While data breaches are not limited to cloud computing, these situations have a dreadful feedback on cloud users. Billions of suggestions were lacking to data breaches in 2017, many of which elaborated cloud servers.

**Table 4.1: Sample Passwords and its ciphertext**

| Slno | Plaintext | Secret key | Ciphertext |
|---|---|---|---|
| 1 | welcome | Network | Otsrestu |
| 2 | TrustEveryone | Computer | Eabzerwtaxmlrw |
| 3 | IloveYou | World | Krboklwv |
| 4 | Dragonball%56 | Keyword | addhescbizl↕iz |
| 5 | Freedom@123 | India | Esfwleholhih |
| 6 | PasSwoRd for Laptop | Virus | mdrzizxcedhmcxfemypq |
| 7 | Symbols not in use | Blog | Txiogogtgsvmpkqtmo |
| 8 | Numerical values | Diamond | Fdocqabmhowifyct |
| 9 | Hello World | Computer | Fanwwewomekf |
| 10 | Diamblosecu | Security | Ldbimpecuw |

In the playfair cipher the numbers and symbols are also encrypted and it store in the server. The data breaches are major problems in the cloud computing security. Table 4.1 gives some sample passwords and its encrypted text.

### 4.2 Results of Ceaser Cipher

Even the highest progressive cloud security can't assure against hustle when testimony swindler have arrangement contact. Unfortunately, unjustified contact is a denoting controversy. Framework of every bigness indicate a absence of expandable existence access administration arrangement breakdown to use multi-factor confirmation, weak keywords use, and a lack of on-going power-driven alternation of cryptographic keys, and certificates. Yao et al., described in the research article about the cloud users and the security unions should scrutiny the slender data loss necessities, ask about the severance of a provider's solution, and separate to which entity is involved for data loss and under performs. Some providers afford solutions for geographic redundancy, data backup within the cloud, and premise-to-cloud backups. The hazard of relying on the provider to store, backup and keep the data must be directed against management that purpose in cloud. The choice to do both may be made if data is extremely grave and cloud users are covering the data loss and file theft problems. In this paper the substitution technique is providing additional security to cloud users. The Secret key will be used to encrypt the passwords and data will be secured in the cloud server. The data loss will be reduced and data will be protected using secret key[26]. The figure 4.6 is shown how the password will be encrypted and decrypted in the ceaser cipher.


**Figure 4.6: Ceaser cipher using characters and numbers**

In this example the ceaser cipher algorithm are designed to protect user data. In this figure 4.6 shown the plain text does not encrypt blank space and special characters. It accepts numbers and alphabets using that word and made decryption according to it.


**Figure 4.7: Ceaser cipher using special characters.**

Figure 4.7 showing the example of ceaser cipher and data decrypted according to the plain text. Hence the special character didn't decrypted by ceaser cipher. The user uses the cipher according to the needs.

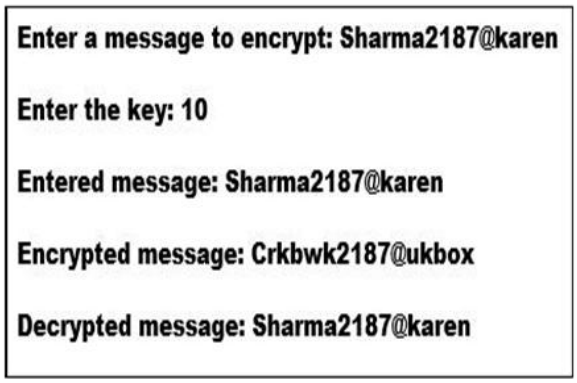


**Figure 4.8: Result of Ceaser cipher**

The ceaser cipher accepts all characters and numbers except special characters. The data protected according to the user possibility. The combination of numbers and characters are used as a password in the Figure 4.8.

**Table 4.2: Sample Passwords in ceaser cipher**

| SLNO | Plaintext | Secret key | Ciphertext |
|---|---|---|---|
| 1 | Welcome | 4 | Aipgsqi |
| 2 | TrustEveryone | 4 | Xvywxizivcsri |
| 3 | IloveYou | 10 | Svyfoiye |
| 4 | Dragonball%56 | 7 | Kyhnvuihss%56 |
| 5 | Freedom@123 | 5 | kwjjitr@123 |
| 6 | PasSwoRd for Laptop | 6 | Vgyycuxj lux rgvzuv |
| 7 | Symbols not in use | 8 | Lrfuhel ghm bg nlx |
| 8 | Numerical values in the list | 5 | Szrjwnhfq afqzjx ns ymj qnxy |
| 9 | Hello World | 8 | Pmttw ewztl |
| 10 | Diamblosecu | 7 | Kphtisvzljb |

In the Ceaser cipher the data breaches problems are highly focused. The data breaches problem is main issues in the cloud computing server. The security of Ceaser cipher is very low compare to playfair cipher. Table 4.2 gives some sample passwords and opted cipher text. The cipher text only stored in the cloud database.

### 4.3 Discussion

In the cloud computing security target scrap to determinate is data breaches. In this research article separate two processes is ceaser and playfair methods. By observe playfair and ceaser algorithm, Playfair algorithms are inimitable to occasion and providing giant immunity to cloud users and cloud providers.

Over the past year, Google has fingered to rope in an enormous quantity of Indian enterprises to the paid Google Cloud Platform. The absorption primarily on the partner-based kind and have combined with many inclusive and Indian sovereign software merchants to offer our solutions. Apart from this, Google has added a new package called Cloud Spanner

[27]. Y. Chen, et al., discusses expertise foremost also hypothesises that with more statement of cloud there is a need for proficient expertise in the administrative district. It has concert with Coursera, a leading spheric online improvement stage, to eject a streak of on-demand Google Cloud Platform training penitence that will also help in progress of cloud services in the nation in the research paper What's New About Cloud Computing Security [28]. Table 4.1 is shown about Indian public cloud service.

**Table 4.1: Different kind of cloud users**

| India Public Cloud Services Forecast(in $ million) | | | | | | |
|---|---|---|---|---|---|---|
| **Years** | **2015** | **2016** | **2017** | **2018** | **2019** | **2020** |
| BPaas | 92.5 | 114.3 | 146.9 | 188.8 | 242.4 | 311.5 |
| SaaS | 299.3 | 389.8 | 514.4 | 654.2 | 792.4 | 959.6 |
| PaaS | 62.4 | 82.1 | 106.9 | 135.0 | 160.4 | 184.7 |
| IaaS | 33.89 | 448.9 | 615.4 | 839.7 | 1140.6 | 1558.0 |
| CMSS | 79.4 | 104.2 | 134.5 | 167.7 | 206.2 | 247.8 |
| Cloud Advertising | 95.6 | 123.5 | 158.0 | 189.0 | 222.8 | 266.0 |
| Total | 968.1 | 1262.6 | 1676.2 | 2174.3 | 27647.7 | 3527.66 |

Security enhancement of authenticated RFID generation written by Kamesh and N. Sakthi Priya discussed by security enhancements in the cloud providers and users in the future peers.

The Cloud growth rate surge throughout every year to enlarge the cloud atmosphere figure 4.10 bar diagram shows graphically the growth rate of cloud users. Each and every year the cloud users are increased and cloud providers are providing lot of facility as well as the user needs. The Cloud Business Process Services (BPaaS) business process management are some of the definite publicly vacant employ, whereas there are ordinal of other employ that today IT departments provide to their users within the firewall or to the proved collaborator. The Cloud Application Services (SaaS) oblation types include email

and alliance, Customer relationship management, and healthcare-related claims. Some large creativities that are not conventionally thought of as software vendors have started building SaaS as an additional source of income in order to gain a competitive advantage.

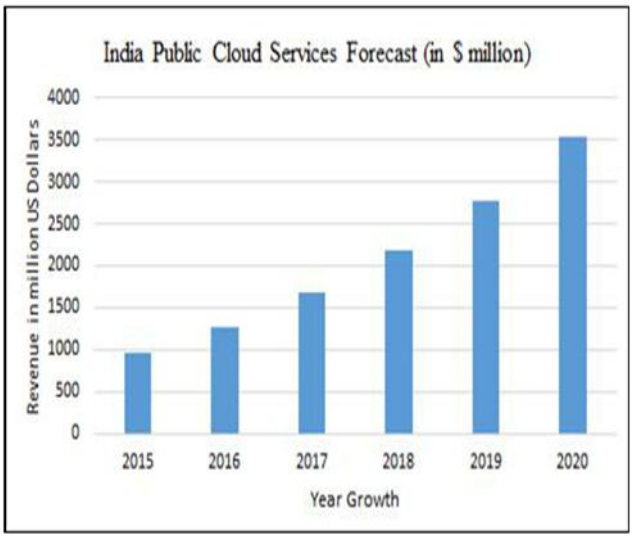


**Figure 4.9: Cloud Growth rate**

## V. CONCLUSION

Cloud computing is comparably advanced approach that accommodate numerous welfare for its end user. However, it also escorts any salvation quandary which may slow down its use. In the various previous research works by many persons, it is converge on redemption doubt and afford one of the elucidations to defended the cloud data and provide appended security for identification to defended the user orientation termed as data breaches. The circumstances will be upheld by employ the secret key in substitution technique and confidential cabinet will be secured by cloud service providers and it will be useful for cloud users. In this research work, it is implemented about two types of substitution techniques ceaser and playfair cipher by means of realizes a usable oriented avenue. The fulfilment of this work is examined by deeper than hundred witnesses and it is determinate from their revision and inspected for the estimation. From the consequence accomplish by this accession, via correlative resolution of two persuasion of cipher, the enforcement of playfair cipher is exceeding to hedge cloud user's orientation than the playfair technique. Also, it converges on its separation and consequences to apprehend the cloud security. Traditional security component may not work well in cloud circumstances because it is a manifold architecture that is possessed an aggregate of particular automation. One of the finest explication designed in the research article is playfair and ceaser cipher. The two ciphers contribute defence to cloud data. According to the user perceptive the security will be chosen by the user. Elaborating rapid estimate to custom cloud data huge salvation for user documents and cloud computing has inherent to incline a contender in subsidize a secure, vital and provident viable IT solution in the future.

## REFERENCES


1. Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I. Above the clouds: A berkeley view of cloud computing. Dept. Ele Eng. and Com. Sci, Uni of Cal, Berky, Rep. UCB/EECS. 2009 Feb 10;28(13):2009.
2. Fernando, N., Loke, S.W. and Rahayu, W., 2013. Mobile cloud computing: A survey. Future gen comp sys, 29(1), pp.84-106.
3. Hayes, B., 2008. Cloud computing. Communications of the ACM, 51(7), pp.9-11.
4. Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18), 1587-1611.
5. Jadeja, Y. and Modi, K., 2012, March. Cloud computing-concepts, architecture and challenges. In 2012 Int Conf on Comp, Electr and Electr Techno (ICCEET) (pp. 877-880). IEEE.
6. Vouk, M.A., 2008, June. Cloud computing—Issues, research and implementations. In ITI 2008-30th Int Conf on Info Techn Inte (pp. 31-40). Ieee.
7. Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Fut Gen comp sys 28, no. 3 (2012): 583-592.
8. Hashem, Ibrahim Abaker Targio, Ibrar Yaqoob, Nor Badrul Anuar, Salimah Mokhtar, Abdullah Gani, and Samee Ullah Khan. "The rise of "big data" on cloud computing: Review and open research issues." Information systems 47 (2015): 98-115.
9. JoSEP, Anthony D., RAnDy KAtz, AnDy KonWinSKi, L. E. E. Gunho, DAViD PAttERSon, and ARiEL RABKin. "A view of cloud computing." Comm of the ACM 53, no. 4 (2010).
10. Ali, M., Khan, S.U. and Vasilakos, A.V., 2015. Security in cloud computing: Opportunities and challenges. Information sciences, 305, pp.357-383.
11. Sun, D., Chang, G., Sun, L. and Wang, X., 2011. Surveying and analyzing security, privacy and trust issues in cloud computing environments. Procedia Engineering, 15, pp.2852-2856.
12. Hussain, Syed Asad, Mehwish Fatima, Atif Saeed, Imran Raza, and Raja Khurram Shahzad. "Multilevel classification of security concerns in cloud computing." Applied computing and info13, no.1 (2107): 57-65.
13. Bhardwaj, A., Subrahmanyam, G.V.B., Avasthi, V. and Sastry, H., 2016. Security algorithms for cloud computing. Procedia Computer Science, 85, pp.535-542.
14. Hairer, Ernst, Christian Lubich, and Gerhard Wanner. Geometric numerical integration: structure-preserving algorithms for ordinary differential equations. Vol. 31. Springer Science & Business Media, 2006.
15. Masetic, Zerina, Kemal Hajdarevic, and Nejdet Dogru. "Cloud computing threats classification model based on the detection feasibility of machine learning algorithms." In 2017 40th Inte Conven on Info and Comm Tech, Electronics and Microelectronics (MIPRO), pp. 1314-1318. IEEE, 2017.
16. Chen, D. and Zhao, H., 2012, March. Data security and privacy protection issues in cloud computing. In 2012 Inter Conf on Com Sci and Elect Engi (Vol. 1, pp. 647-651). IEEE.
17. Basu, S. and Ray, U.K., 2012. Modified Playfair cipher using rectangular matrix. Inter J of Com Appl, 46(9), pp.28-30.
18. Rahim, Robbi, and Ali Ikhwan. "Cryptography technique with modular multiplication block cipher and playfair cipher." Int. J. Sci. Res. Sci. Technol 2.6 (2016): 71-78.
19. Hammood DA. Breaking a playfair cipher using memetic algorithm. J of Eng and Sust Develop. 2013;17(5):172-83.
20. Murali, Packirisamy, and Gandhidoss Senthilkumar. "Modified version of playfair cipher using linear feedback shift register." In 2009 Inter Conf on Info Man and Eng, pp. 488-490.
21. Al-Muhtadi, Jalal F., Abdul Basit, and Maqsood Mahmud. "Development of symmetric cryptosystem using matrices with less overhead on communication channel. Inter Confe on Info and Com Techn, pp. 93-97. IEEE, 2009.
22. Rajput Y, Naik D, Mane C. An improved cryptographic technique to encrypt text using double encryption. Inter j of Com Appl. 2014 Jan 1;86(6).
23. Sun, Y., Zhang, J., Xiong, Y. and Zhu, G., 2014. Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 10(7), p.190903.
24. Berl A, Gelenbe E, Di Girolamo M, Giuliani G, De Meer H, Dang MQ, Pentikousis K. Energy-efficient cloud computing. The com j. 2010 Sep;53(7):1045-51.
25. Rao, R.V. and Selvamani, K., 2015. Data security challenges and its solutions in cloud computing. Procedia Comp Sci, 48, pp.204-209.
26. Yao, Xuanxia, Xiaoguang Han, and Xiaojiang Du. "A lightweight access control mechanism for mobile cloud computing". IEEE 2014 Confe on Comp Comm (INFOCOM WKSHPS), pp. 380-385.
27. Ryan MD. Cloud computing security: The scientific challenge, and a survey of solutions. J of Sys and Soft. 2013 Sep 1;86(9):2263-8.
28. Chen, Yanpei, Vern Paxson, and Randy H. Katz. "What's new about cloud computing security". Univ of Calif, Berk Report No. UCB/EECS-2010-5 January 20, no. 2010 (2010): 2010-5.


## AUTHOR PROFILE

**S. Karthiga,** is a research scholar (full time) under the guidance of Dr. T. Velmurugan in PG and Research Department of Computer Science and Applications, D.G.Vaishnav College, Chennai-600106, India.. And started in research work in cloud computing and its Security Threats. Her current research work focuses on the Security Problems and data breaches in the Cloud Computing. Participated and presented research paper in International/National Conferences and published two journals.

**Dr. T. Velmurugan,** is working as an Associate Professor in the PG and Research Department of Computer Science and Applications, D.G.Vaishnav College, University of Madras, Chennai-600106, India. Also, he is the Head of the Department of Computer Applications (BCA).

He holds a Ph.D. degree in Computer Science from the University of Madras. He elected and served as a Senate Member from Academic Council,University of Madras. He has published more than 100 articles indexed in SCOPUS and SCI such as Applied Soft Computing, Journal of Computer Science and etc. He was an invited speaker of the 10th Int'l Conference on Computational Intelligence and Software Engineering (CiSE 2018) held from January 5-7, 2018 in Bangkok, Thailand. Also, he is a keynote speaker for the same conference to be held on Dec. 13-15, 2019 at Bangkok. He has guided more than 300 M.Phil., Research Scholars in the field of Computer Science. He guided 7 Ph.D. scholars and currently guiding 10 Ph.D. scholars in the same field. He served as a nominated Senate Member in the Middle East University, Dubai, UAE for a period of three years. He is a member in Board of studies for many autonomous institutions and Universities like Periyar University, Salem, India. He hosted a lot of programmes in Doordharsan Television about recent topics in Information Technology. He was an Organizing Secretary of International Conference on Computing and Intelligence Systems (ICCIS 2015) and an international workshop on Applications of IoT. In addition, he was a resource person for various national workshops entitled "Research Article Writing and Journal Publications". He is an editorial board member of many International Journals. He is also a reviewer in many peer reviewed journals like Elsevier, Springer, IOSPress Journals etc. Further, he is a visiting faculty for M.Phil. course for various universities throughout India.