Privacy and Security Aware Cloud Storage using Double Cryptography Method

B. Muthulakshmi, M.Venkatesulu

Abstract: ***Cloud computing, a remote technology that enlightens with several on-demand services. Cloud computing developed with a principle of sharing resources available as per the company needs. Prominent cloud services utilized today are networking, storage, servers, software's, etc. Cloud computing's distributed nature and advanced features create a remarkable footprint in the IT field. It is fair to say without cloud technology the next technical era can't exist. However the cloud computing widely spaced, simultaneous some serious challenges still exists. As per the real-time scenario, there are several challenges still alive, but among which privacy and security are prominent to take concern. Among which the trustworthiness of third-party providers increases the attention on developing an enhanced cloud system. In this paper, we proposed an improved double encryption-decryption (IDED) method for a secure cloud system. The main intention of the proposed work is increasing the privacy and security for the cloud users. The principle applied to the proposed methodology is double encryption and double decryption. The encrypted files are decrypted to view the original data using the keys. These keys are available only to the authenticated users which ensures the system's privacy and security in all manner. The mechanism is processed under the query system of sending and response from the data authority.***

Keywords: Cloud computing, resource sharing, encryption, decryption, data storage, Cloud Service Provider, Data Authority and End User

I. INTRODUCTION

Cloud computing, sharing of resources which are boon for the small as well as middle-level organizations. Organization for small need no need to purchase the entire services. By which they use for their need and pay per use. It is well appreciated for low cost and reliable services in the industry. Currently, it plays a vital role in major domains such as e-transactions, e-commerce, e-billing, e-banking, and e-mail. Due to the increasing features, the vast amount of user's using cloud computing as a major component for their business. This maximizes the possibility of network traffic among the users and cloud servers. The primary thing needed for these services is online data transmission [1-2].In the industry, third party service providers are increased quietly. This creates the security and privacy issues among the users especially data leakage or data loss. Generally, most of the clients are storing their sensitive data in cloud storage, it has maximum security but therefore several threats still exist [3-5].

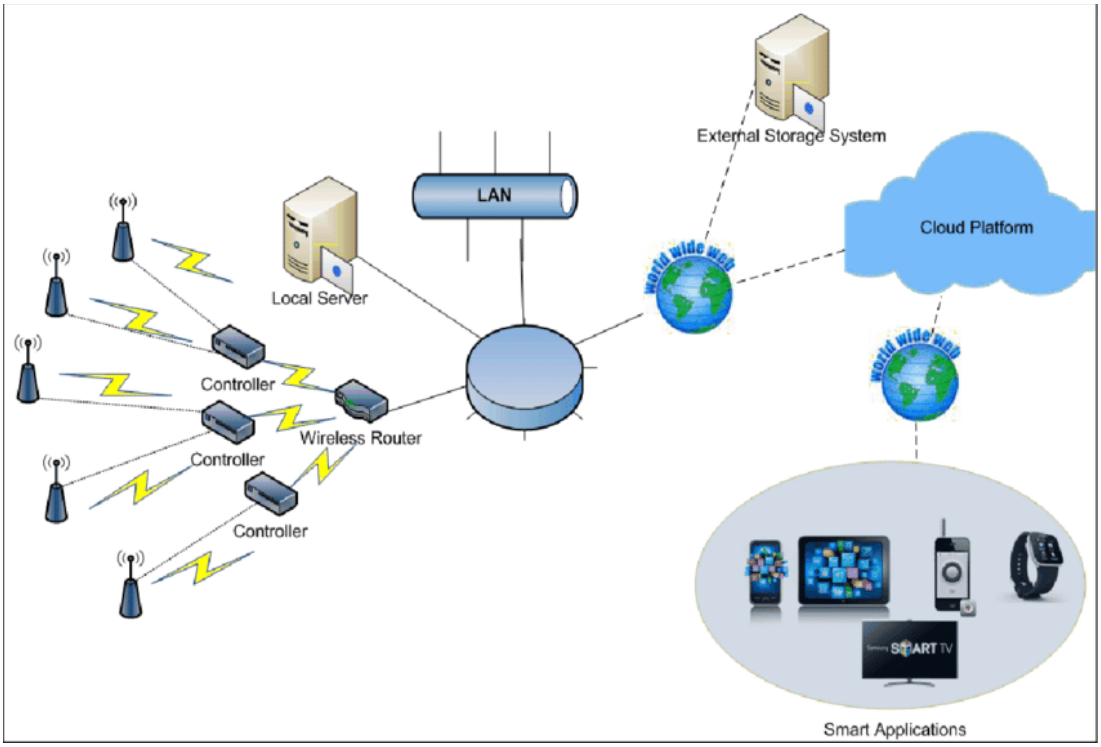

Fig 1: Simple Cloud Computing System

Revised Manuscript Received on December 05, 2019.

B. Muthulakshmi*, Department of Computer Applications, Kalasalingam University, Krishnankoil, Tamil Nadu,India.
M. Venkatesulu, Department of Information Technology, Kalasalingam University, Krishnankoil, Tamil Nadu, India.
*Corresponding Author: selvamayil2010@gmail.com

The above fig1 shows how cloud computing connects and working with smart applications through the internet or any wireless media On cloud computing, there are three models of services such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) [6-7]. Iaas is a service of raw computing hardware such as servers or storage. It is also known as utility computing that is buy what you need and pay-as-you-go concept. Paas platform-based services are well applicable for the programmers and developers. Their web-based tools are available where you can run the software and hardware which are provided by other companies. SaaSservice is well known as application services, a real-time example such as Web-based email and Google Documents. The famous cloud service providers in the industry are as follows:

- Google Cloud
- Microsoft Azure
- Amazon Web Services (AWS)
- IBM Cloud
- Aliyun
-

The cloud computing architecture consists of two main components along with two subcomponents. The two main components are the front-end platform and back-end platform. The front-end platform combines of clients and other mobile devices. The back-end platforms are such as servers and storage systems. The subcomponents are Cloud-based delivery and network (internet, intranet). The user interacts by the front end where the cloud processing is done at the back end through the web components like Cloud-based delivery and network. In the cloud system, the major part is performed by Cloud Service Providers (CSP). The main responsibility of the CSP is obtaining the request from the user and checking the authentication by the user profile. The access is provided to the user. They can store their files, alter or delete, the major issue is security and privacy. The users are suffering from data integrity issues as they are storing their data in a remote location. For which cryptography is introduced in cloud computing. Cryptography is the process of changing the plain text into cipher text. It is the mechanism of encrypting and storing the data in the cloud. Employing the valid key to the authorized user, they can decrypt and view the original file. There are two kinds of secret key generation such as symmetric and asymmetric. Symmetric key generation is the process of using a private key and only one key for the cryptography algorithm. The famous symmetric key generationalgorithm available in the industry is theData Encryption Standard (DES) and Advanced Encryption Standard (AES). Whereas asymmetric key generation is the special kind of process with two keys such as public key and private key. The most commonly used asymmetric key generation algorithms are RSA and Elliptic Curve Cryptography (ECC) [8-13].

This paper is organized as follows; the introduction is discussed in section 1. Section 2 contains related works. Section 3 with the problem statement. In section 4 our contribution is described. Section 5 comprises of proposed design architecture, algorithm, and mechanism of the workflow.

II. RELATED WORK

DiaaSalamaAbdElminaam et al [14] proposed a new hybrid technique for Cryptography. This architecture combines both symmetric as well as asymmetric algorithms such as (AES and Blowfish). The main purpose of this combination is increasing the security level. Here MD5 hashing function is used for hashing the key in encryption and decryption process which enables multiple people to process at the same time.

Acqueela G Palathingal et al [15] proposed combined encryption and steganography methods for increasing the security level in cloud storage. The concept of this mechanism is data are encrypted and stored behind the images. As an image it is stored in the cloud, on the point of the attacker, it is image as the data are secured. The authenticated user downloaded the image, employing the provided key they can decrypt the file to get the original data behind the image.

Mohammad UbaidullahBokhari et al [16] proposed Data Encryption and Decryption Using K-NN Machine Learning. In this work, the author concentrated on minimizing the time and power required for encryption as well as decryption. Initially, the author segregates the stored data in the cloud as normal sensitive or highly sensitive. Based on the sensitive level the authentication is provided to the user. For highly sensitive data AES-256 algorithm is used with RSA (Rivest–Shamir–Adleman) algorithm for encrypting the key of AES 256. For normal sensitive data AES (advanced encryption standard)-192 algorithm is applied.

DhuratëHyseni et al [17] proposed an advanced model to Increase the Security of Sensitive Data in Cloud Computing. The approach is mainly designed for companies and organizations. This method encloses with efficient key management and access permissions systems. It segmented before encryption on decryption correction combination gives a successful result. Here the attacker fails to combine all the segmented files.

Hitesh Marwaha&Rajeshwar Singh et al [18] proposed Data Sanitization and MAC address based AES. The principle behind this process is finding the sensitive data before transmission to the cloud and implementing mac address dependent AES technique for non-sensitive data. By this mathematical approach of data, sanitization does not show sensitive data as it is. That is it fools the attackers as non-sensitive data.

Disadvantages of related works:

At [14] it enables multiple private keys for several users at the same time which leads to trafficAt [15] the storing of data behind the images increases the computational cost. The storing of data in the pixel has the possibility of data loss or sometimes leads to the collapse of stored data in the cloud.

At [16] it is not fair to state the sensitive level, as on user point every data they are storing in the cloud is highly sensitive. At [17], here the process of segmentation is too crucial for the user itself. As the data are stored in a remote location, it is not fair to guarantee that were all the segmented files stored in cloud storage. Sometimes on the increasing number of segmentation results in huge file separation,

which means the entire file can't be obtained as decryption is not possible. At [18], it is not guaranteed that the attackers will hack the sensitive data only. Utilizing false sanitization on sensitive data, it is not entirely safe, that is there is a maximum possibility that the hacker uses the non-sensitive data also.

III. PROBLEM STATEMENT

In the increasing technical advancement simultaneously several threats are also increased. The major factors which are needed to maintain the security and privacy of the cloud system are as follows: Authentication, Authorization, Integrity, Audit, and Availability.

- **Authentication**: Preventing unauthorized users to access or visit the site/network. It can be done by data checking at the cloud services provider validating the user's credentials.
- **Authorization:** Accessible for only authorized users
- **Integrity**: Data validity checking on the date of stored data until it gets any modification without the data owner's acknowledgment. At the same time checking any data lost during transmission.
- **Audit**: Automatic system valuation on information security.
- **Availability**: Proper maintenance of information or data.

Also, we have discussed in related works, some of the cryptographic approach also not efficient in marinating the security of user data. This enables more interest in developing a higher level of enhancement in maintaining cloud security. This motivation leads to the development of our proposed work. Let's discussed our proposed methodology, architecture, algorithm, and workflow detail in the upcoming sections.

IV. OUR CONTRIBUTION

In this paper, initially, we have analyzed the various security threats which still exist such as Data rupture, Hijacking of the user account, Internal attacks, Malware implantation, Denial of service attack (DoS) and Loss of cloud data. Next, the various existing method used for maintaining cloud security such as, K-NN, hybrid cryptography, E-S methodology, etc along with their disadvantages and what makes these approaches failures. Based on this deep analysis with the real-time scenario our proposed work is designed and developed in maintaining the security and privacy in the cloud storage system.

V. PROPOSED METHODOLOGY

Data Authority: The data authority is responsible for the collections of various data like text, images, audio and video from several sources. Data authorities took control of marinating the data according to the appropriate user by labeling or indexing. Then checking with the user credentials and requesting end users. The data and verification are a success then the user is awarded as authorized user who can all the rights to access the stored data in the cloud.

Cloud Storage: Cloud storage is a distributed service that is allowed by cloud service providers (CSP). Employing then and the internet, the user can be stored and retrieve their data. Nowadays several third-party cloud providers are available in the markets, most of them in a remote location. They were very popular due to their attractive packages along with affordable services on cost, availability, confidentiality, and reliability. The popular cloud providers in the industry are Sun Cloud, Windows Azure services platform Amazon's S3 and Amazon Elastic Compute Cloud (EC2).

Cloud Service Provider (CSP): The CSP is taking over responsibility for allocating the space for the authorized users. In other ways, CSP has to manage the control of computational resources. They received the request from the user, validating the user accessible and responsive to the user. The CSP took over the control on a server as well as the storage on the cloud system.

End Users: The end user **is** more important in the cloud system**,** the services are to be provided as per their needs. It fair that all cloud services meet the reliability, accessibility, and security in all manner. These end users are permitted to store their data in their allocated spaces. By proving them as an authorized user they can edit, alter and restore the files in the cloud system.

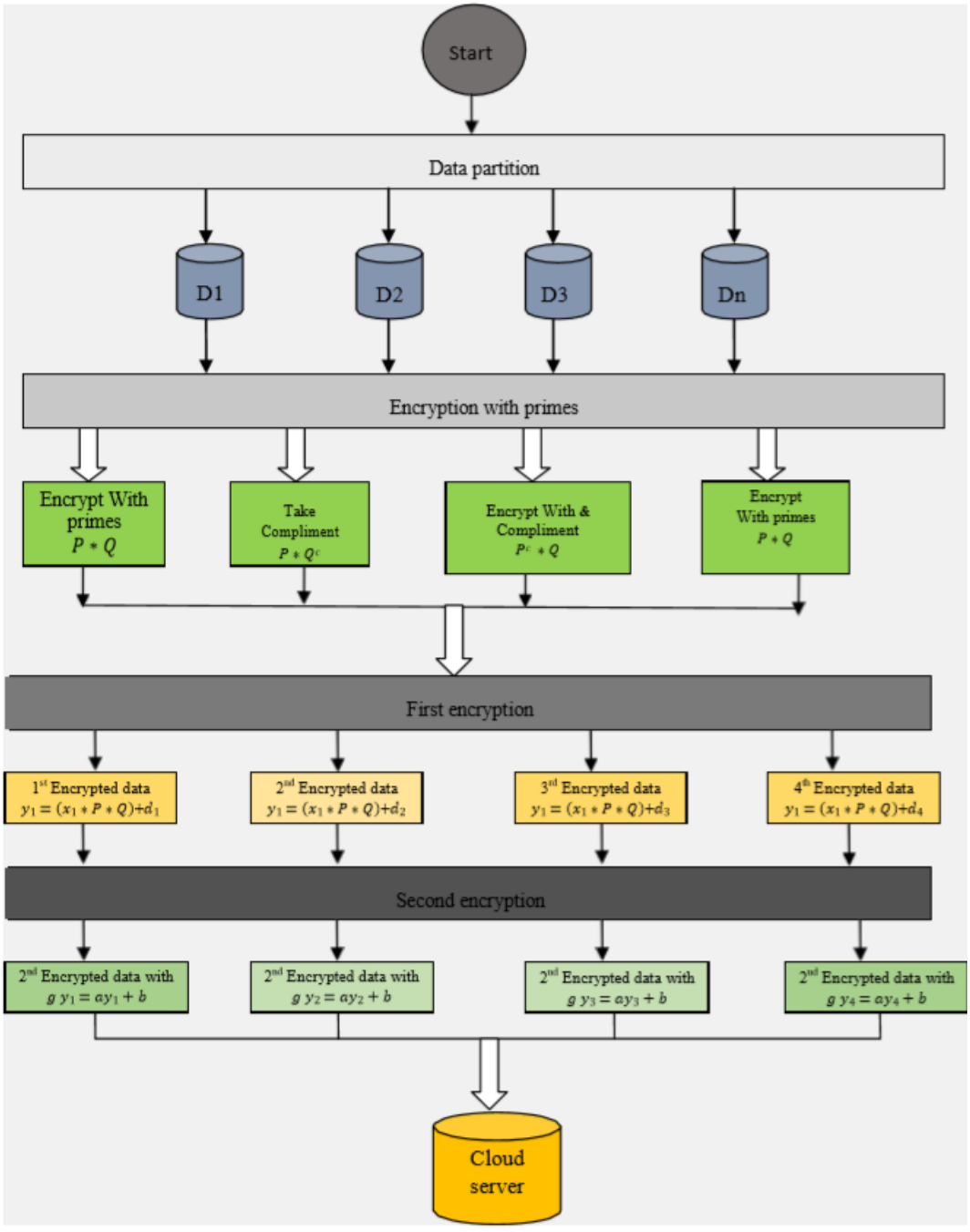

Figure 2: Proposed encryption architecture

Algorithm for proposed architecture

1. *Begin ();*
2. *Start the encryption process;*
3. *Initialize the data partition and distribute the plain text* $P \rightarrow t_1, t_2, t_3 .. t_n$
4. *Generate the prime number* P_{xi} *and* $P_{xi} = 2X_i$
5. *Take sorting of* P_{xi} $(Q_i$ *and* $R_i)$
6. *Takes the complement of prime* P_{xi} $Q^{ci}{}_i$, $R^{ci}{}_i$
7. $Cipher K^{ci}{}_i = 2^{p+1} - K_i$;
8. $Generate random integer I = d_1 + d_2 + d_3 \ldots d_n$
9. $I_n = x_n$ *we have taken* $N = 4$;
10. *Case(i)*
11. *Encrypted data*
12. *First encrypted data*
13. (i) $y_1 = (x_1\ Q_i * R_i\ + d_1)$
14. (ii) $y_2 = (x_1\ Q_i * R^{ci}{}_i\ +\ d_2)$
15. (iii) $y_3 = (x_1\ Q^{ci}{}_i * R_i + d_3)$
16. (iv) $y_4 = (x_1\ Q^{ci}{}_i * R^{ci}{}_i + d_4)$
17. *case 2*
18. (i) $g(y_1) = a\, y^2{}_1 + b$
19. (ii) $g(y_2) = a\, y^2{}_2 + b$
20. (i) $g(y_3) = a\ \ y^2{}_3\ \ + b$
21. (i) $g(y_4) = a\ \ y^2{}_4\ \ + b$
22. *End*

Working principle

Initially, the data partition is processed in our proposed methodology. The data partition is very important, as data are collected from various sources in different formats like text, images, audio, and videos. This partition saves a lot of time in total processing. As our proposed mechanism is of double time encryption and double decryption, the first level of encryption is carried out. For this prime number is generator with it a compliment and based on that terminology all data are get encrypted. The second level of encryption is done using an invertible non-linear function which applied to the encrypted data. Then the double encrypted file is stored on different locations on the cloud storage system. The double encryption is expressed as below;

$$y(x) = px + q$$

Where and q are integers and x is the ciphertexts produced by the first encryption. To perform second encryption, each cipher partition is multiplied by p and added with q.

Then the decryption process is carried out, the end user who needs to get their stored files from the cloud sends a request to the data authority or CSP. Based on that they processed the authentication after verified by the CSP the end user allows to access their files. The obtained files from the multiple locations are merged and decrypted double time using the double secret keys provided to them. The expression for decryption is stated below;

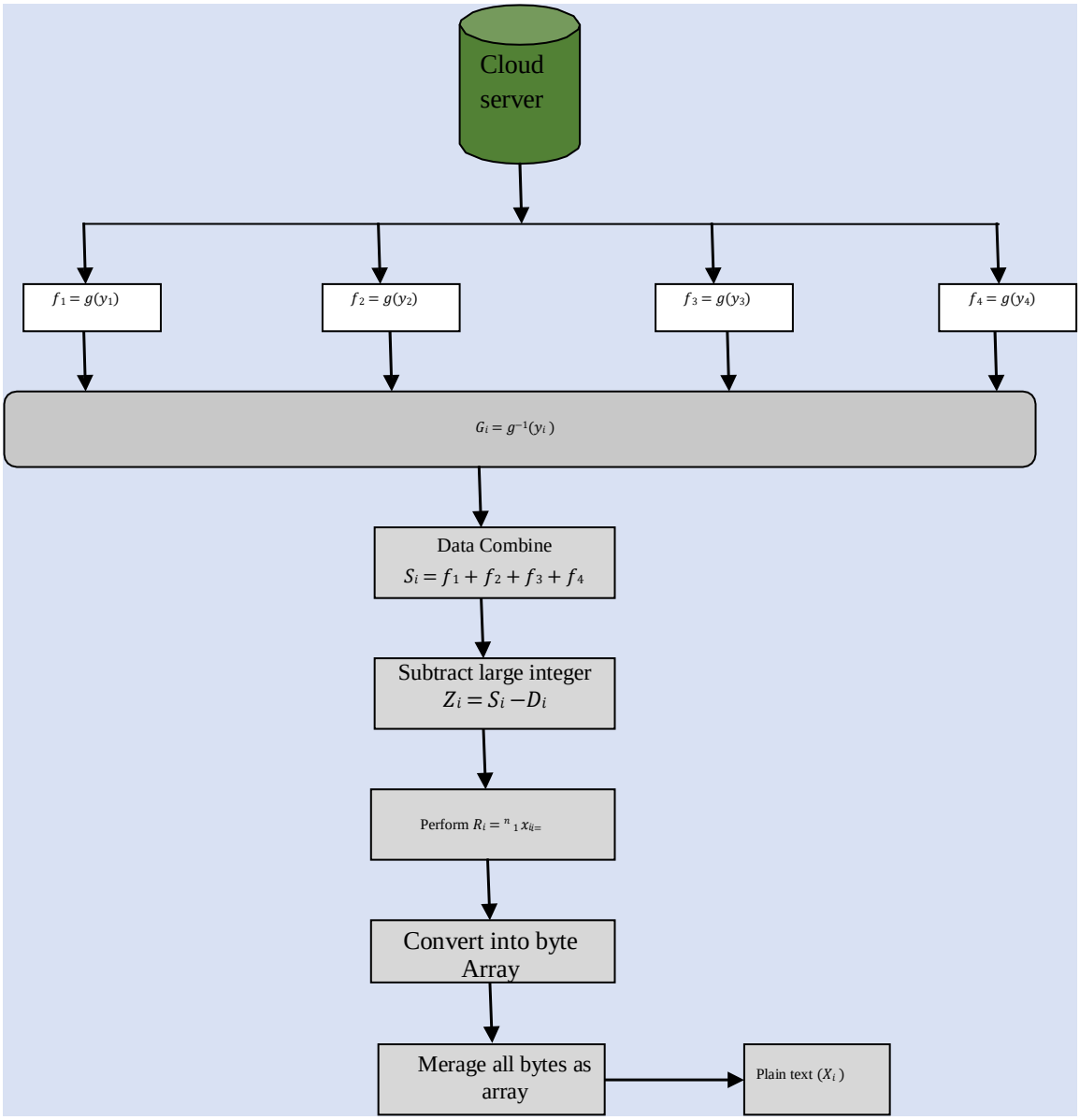

Figure 3: proposed decryption architecture

$$y^{-1}(x) = \frac{x_i - q}{p}$$

Where and q are integers and x is the data partition.

Algorithm for decryption

1. Step-1 Apply inverse from INF
2. $G = g^{-1}\ y = \frac{y_i - b}{a}$
3. Step-2 encrypted chipper text
4. $f_1 = g(y_1^2)$;
5. $f_2 = g(y_2^2)$;
6. $f_3 = g(y_3^2)$;
7. $f_4 = g(y_4^2)$;
8. Step-3 add all encrypted chipper text
9. $S_i = f_1 + f_2 + f_3 + f_4$;
10. Step -4 subtract larger integer
11. $Z_i = S_i - I_i$
12. Delete zero pads
13. Step-5
14. Perform the above steps on all the four encrypted data parts (up to n x) and sum all of them.
15. Step 6: Convert into byte array
16. Step 7: Merge all Byte arrays
17. Step 8: Get original plaintext ( )

The proposed mechanism work in the principle of fooling the attackers. Even though the attacker hacks the stored files he not sure about the original data. Even though they encrypt the data, due to double encryption-decryption the possibility of data secure is maximum compared to the existing technologies.

VI. CONCLUSION

In this paper, several causes and issues in cloud security are analyzed. Based on the drawbacks of the existing algorithm, we proposed a double encryption-decryption mechanism in our proposed system known as IDED. The proposed mechanism working principle is fooling the attackers. Even though the attacker hacks the stored files he not sure about the original data. Even though they encrypt the data, due to double encryption-decryption the possibility of data secure is maximum compared to the existing technologies.. Data are collected from various sources on different formats and stored on the cloud. Before storing, it undergoes double encryption and on retrieving double decryption to get the original data.

REFERENCES

1) C. Xue-Zhou, “Network data encryption strategy for cloud computing,” in 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, Nanchang, 2015, pp. 693–7.
2) Fadhil Salman Abed, “A Proposed Method of Information hiding based on Hybrid Cryptography and Steganography”, International Journal of Application or Innovation in Engineering & Management, Vol. 2, Issue 4, April 2013.
3) B. Hauer, “Data and information leakage prevention within the scope of information security,” IEEE Access, Vol. 3, pp. 2554–65, Dec. 2015.
4) G. Sweetha, K. Suriya, and R. Jothi, “Security and privacy issues in cloud computing,” Emerg. Trends Adv. Comput., pp. 69–75, 2015.
5) L. Tawalbeh, N. S. Darwazeh, R. S. Al-qassas, and F. Aldosari, “A secure cloud computing model based on data classification,” Procedia – ProcediaComput. Sci., Vol. 52, pp. 1153–8, Jun. 2015.
6) Shekokar N, Sampat K, Chandawalla C, Shah J (2015) Implementation of fuzzy keyword search over encrypted data in cloud computing. In: Proceedings of international conference on advanced computing technologies and applications (ICACTA- 2015) held in Mumbai, India, ISBN: 978-1-5108-0136-3, vol 45. pp 499–505.
7) Singh R, Kumar S, Agrahari SK (2012) Ensuring data storage security in cloud computing. IOSR J Eng 2(12):17–21
8) L. Abusalah, A. Khokhar, M. Guizan, \A survey of secure mobile ad hoc routing protocols," IEEE Communi- cations Surveys & Tutorials, vol. 10, no. 4, pp. 78-93, 2008.
9) S. Haykin and M. Moher, Modern Wireless Communication, Prentice Hall, 2005.
10) G. J. Pottie and W. J. Kaiser, \Wireless integrated network sensors," Communications of the ACM, vol. 43, pp. 51-58, 2010.
11) Ajit Singh, AartiNandal and Swati Malik, “Implementation of Ceaser Cipher with Rail Fence for enhancing data Security”, International Journal of Advanced research in Computer Science and Software Engineering. Vol 2, Issue 12, December 2012 pp. 78 -82.
12) Amit joshi and Bhavesh Joshi “A Randomized Approach for Cryptography” International Conference on Emerging Trends in Network and Computer Communications (ETNCC), April 2011, pp. 293- 296
13) SomdipDey “SD-AREE: An Advanced Modified Ceaser Cipher Method to Exclude Repetition from a Message” International Journal of Information & Network Security (IJINS). Vol. 1, Issue. 2, June 2012, pp. 67-76
14) DiaaSalamaAbdElminaam,"Improving the Security of Cloud Computing by Building New Hybrid Cryptography Algorithms"., I.J. of Electronics and Information Engineering, Vol.8, No.1, PP.40-48, Mar. 2018 (DOI: 10.6636/IJEIE.201803.8(1).05)
15) Acqueela G Palathingal, Anmy George , Blessy Ann Thomas and Ann Rija Paul,” Enhanced Cloud Data Security using Combined Encryption and Steganography”, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072.
16) Mohammad UbaidullahBokhari, QahtanMakkiShallal and YahyaKordTamandani, "Reducing the Required Time and Power for Data Encryption and Decryption Using K-NN Machine Learning" IETE JOURNAL OF RESEARCH, 2018 https://doi.org/10.1080/03772063.2017.1419835
17) DhuratëHyseni, BesnikSelimi, ArtanLuma and BetimCico, "The Proposed Model to Increase Security of Sensitive Data in Cloud Computing", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.9, No. 2, 2018
18) Hitesh Marwaha and Rajeshwar Singh, "The Secure Migration of Data to Cloud using Data Sanitization and MAC address based AES". International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7, Issue-6, March 2019