International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

ECS: An Enhanced Cloud Security Algorithm

J. Charles Selvaraj, V. Arul Kumar, V. Francis Densil Raj, A. Dalvin Vinoth Kumar

Abstract - Cloud computing is a technology where it provides software, platform, infrastructure, security and everything as a service. But this technology faces many security issues because all the data or information are stored in the hands of the third party. The cloud users unable to know where the data are store in the cloud environment and also it is very difficult to analyze the trustworthiness of the cloud service providers. In this technology providing security is a very big challenging task. This challenge was overcome by developing different cloud security algorithms using cryptographic techniques. Recently many researchers identified that if the cryptographic algorithms are combined in a hybrid manner it will increase the security in the cloud environment. Even though, many research works are still carried out to improve security in the cloud computing environment. In this research article, a new step was taken to develop a new cloud security algorithm

Index Terms: Cloud Security, Cryptographic Cloud Storage

I. INTRODUCTION

Distributed computing is web based registering which is utilized to share the assets, programming, and data. This innovation is entirely adaptable for the clients since they need to pay just for the utilized assets. In this innovation, it offers the accompanying three significant administrations [1].

1. Software as a Service(SaaS)
2. Platform as a Service(PaaS)
3. Infrastructure as a Service(IaaS)

A. Software as a Service(SaaS)

It is a product dispersion model in which an outsider supplier has applications and makes them accessible to clients over the Internet.

B. Platform as a Service(PaaS)

It conveys equipment and programming instruments for the most part those required for application improvement to clients over the web.

C. Infrastructure as a Service(IaaS)

It gives virtualized processing assets over the web

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Dr. J. Charles Selvaraj*, Department of Computer Science, Arignar Anna Govt. Arts College, Musiri, India
Dr. V. Arul Kumar, School of Computer Science and Applications, REVA University, Bangalore, India
V. Francis Densil Raj, School of Computer Science and Applications, REVA University, Bangalore, India Fourth Author
Dr. A. Dalvin Vinoth Kumar, School of Computer Science and Applications, REVA University, Bangalore, India Fourth Author

II. CLOUD DEPLOYMENT MODELS

The distributed computing offers four sending models

1. Private Cloud
2. Public Cloud
3. Hybrid Cloud
4. Community Cloud

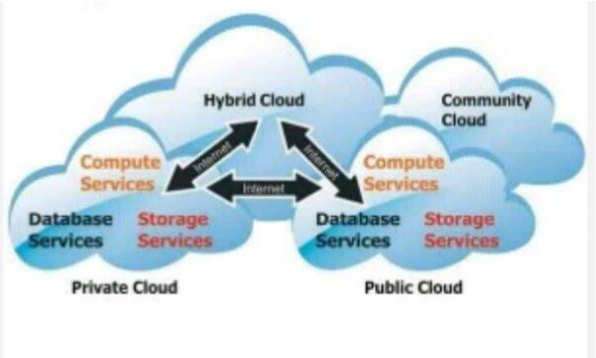

Fig 1. Cloud Deployment Models [2]

A. Private Cloud

The cloud framework is provisioned for selective use by a solitary association involving various customers. It might be claimed, overseen, and worked by the association, an outsider, or a mix of them, and it might exist on or off premises [3].

B. Public Cloud

The cloud foundation is provisioned for open use by the overall population. It might be possessed, overseen, and worked by a business, scholastic, or government association, or a mix of them. It exists on the premises of the cloud supplier [3].

C. Hybrid Cloud

The cloud foundation is a piece of at least two particular cloud frameworks (private, network, or open) that stay remarkable substances however are bound together by institutionalized or exclusive innovation that empowers information and application versatility [3].

D. Community Cloud

The cloud framework is provisioned for selective use by a particular network of shoppers from associations that have shared concerns. It might be claimed, overseen, and worked by at least one of the associations in the network, an outsider, or a mix of them, and it might exist on or off premises [3].

III. CHARACTERISTICS OF CLOUD COMPUTING

The distributed computing innovation gives different administrations to the cloud clients and these administrations are set up both industrially and mechanically, it will cause the organization to improve their potential advantages.

These things are accomplished by the accompanying five significant qualities of distributed computing

A. On-request Self-administration

Distributed computing assets can be provisioned without human collaboration from the specialist organization. As it were, an assembling association can give extra registering assets as required without experiencing the cloud specialist co-op. This can be an extra room, virtual machine cases, database occurrences, etc [4].

Assembling associations can utilize a web self-administration gateway as an interface to get to their cloud records to see their cloud benefits, their use, and furthermore to arrangement and de-arrangement benefits as they have to.

B. Broad Network Access

Distributed computing assets are accessible over the system and can be gotten to by various client stages. It different words, cloud administrations are accessible over a system—in a perfect world high broadband correspondence interface, for example, the web, or on account of private mists it could be a neighborhood (LAN).

System transfer speed and inactivity are significant parts of distributed computing and expansive system get to in light of the fact that they identify with the nature of administration (QoS) on the system. This is especially significant for serving time-delicate assembling applications [4].

C. Multi-tenure and Resource Pooling

The assets of distributed computing are intended to help a multi-inhabitant model. Multi-tenure enables different clients to have similar applications or the equivalent physical framework while holding protection and security over their data. It's like individuals living in a loft building, having a similar structure framework yet despite everything they have their very own condos and security inside that foundation. That is the means by which cloud multi-tenure works.

Asset pooling implies that various clients are adjusted from the equivalent physical assets. Suppliers' asset pool ought to be huge and adaptable enough to support different customer necessities and to accommodate economy of scale. With regards to asset pooling, asset distribution must not affect exhibitions of basic assembling applications [4].

D. Rapid Elasticity and Scalability

Capacities can be flexibly provisioned and discharged, now and again consequently, proportional quickly outward and internal proportionate with interest. To the customer, the capacities accessible for provisioning frequently seem, by all accounts, to be boundless and can be appropriated in any amount whenever [4].

E. Measured Service

Cloud frameworks naturally control and streamline asset use by utilizing a metering capacity at some dimension of deliberation suitable to the kind of administration (e.g., capacity, preparing, data transfer capacity, and dynamic client accounts). Asset use can be checked, controlled, and announced, giving straightforwardness to both the supplier and buyer of the used administration [4].

IV. CLOUD SECURITY

Cloud computing technology shares all the computing resources through the internet. And these resources are offered to the customers as a service through various technologies. Hence, this security is one of the biggest challenging issues. Because all the data are stored in the third party service provider and this becomes an obstacle for implementing the cloud computing techniques. Nowadays, usage of cloud environment gets increased and the data stored here should be in a secured manner [5].

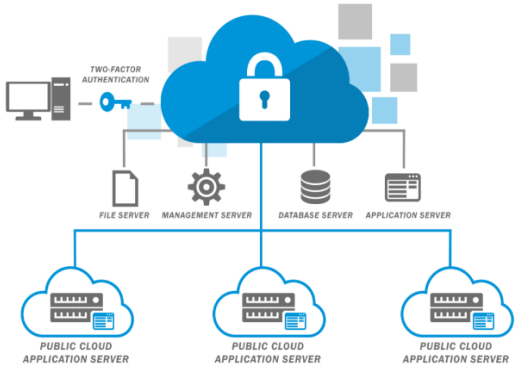

Fig. 2. Cloud Security [6]

V. CRYPTOGRAPHIC CLOUD STORAGE

In the cloud, environment data are stored in a remote location and it is not known to the cloud users. If the data are not stored in a secured manner, there may be a chance of disclosing or modification of the user's data. To show the trustworthiness of the data a secured storage is required. This can be achieved by adopting the cryptographic technic to store the data. In this mechanism, the data are encrypted on the user side and then it will be uploaded to the cloud environment. The following figure clearly shows the mechanism of the secured storage [7].

A. Advantages of Cryptographic Cloud Storage

- **Confidentiality**: It is the concept of ensuring that data is not made available or disclosed to unauthorized people. It is achieved through strong encryption algorithms. Both symmetric and asymmetric encryption algorithms that cannot be easily "broken." If the data is confidential, it cannot be read or understood by anyone other than the intended recipient or recipients [7].
- **Integrity**: It is a term of data security, is nothing but the guarantee that data can only be accessed or modified by those authorized to do so, in simple word it is a process of verifying data. As data integrity gives the guarantee that data is of high quality, correct, unmodified [7].

VI. LITERATURE REVIEW

In this research article a cloud security algorithm was proposed to improve the security in the cloud storage. In this algorithm two different cryptographic techniques AES and Blowfish are used in the hybrid manner.

This algorithm is compared with the existing cloud security algorithms and it shows the improved result [8].

Majedah Alkharji and Hang Liu developed the security algorithm for the cloud environment. In this they developed the algorithm using the homomorphic cryptographic algorithms. This technique allows the user to encrypt their data. In this algorithm different mathematical techniques were adopted. This algorithm provide security for the users' data in the cloud environment [9].

Diksha Gupta et. al, surveyed the various cloud security issues. Nowadays many organizations are transforming the data into the cloud environment. So there is a need to protect that user data against various attacks. Hence, they developed cloud security using the cryptographic techniques. This algorithm improves the security in the cloud storage [10].

Gangolu Sreedevi et al. developed a new security algorithm for the data storage in the cloud storage system. In this algorithm they are not encrypting the whole message. They are splitting the entire message into smaller units and they were encrypting the message unit by unit and for verification some metadata is used. This algorithm was compared with the existing ones and it shows the improved security in the cloud environment [11].

VII. PROPOSED METHODOLOGY

In the cloud environment providing security to the data is one of the biggest challenging task. This challenge can be overcome by applying various cryptographic techniques in a hybrid manner. Recently, many researchers developed cloud security algorithms. Even though, the cloud environment required improvement. Hence in this research a new cloud security algorithm is proposed by combining two cryptographic algorithms to enhance the cloud security.

A. MRC6 Algorithm

This algorithm was implemented by modifying the existing RC6 algorithm. In this MRC6 algorithm it can able to handle 512 bits of input block. This was achieved by enhancing the four 32 bit registers are increased by sixteen 32 bit registers. This MRC6 provides better security for the data [12,13].

B. TORDES Algorithm

This algorithm was developed to provide better security for the user data. It is block cipher algorithm which transforms the strings byte by byte. This transformation was done using two different stacks and a lookup table. The first stack used for making different combination of strings and the second stack used for various combination of delimiter. Finally, the lookup table contains the code words of the corresponding operators which are present in the first stack. By this encryption and decryption process were carried out. This algorithm protects the user data form the various attacks [14].

C. Enhanced Cloud Security (ECS) Algorithm

The ECS algorithm is proposed by integrating two existing cryptographic algorithms. This algorithm improves the security in the cloud environment. The ECS algorithm consist of 64-bit key and 512-bit Input String and in this two cryptographic algorithms are combined in a hybrid manner. The ECS algorithm is developed and deployed to the cloud environment and it will be provided to the users as a cloud security service.

STEP 1: Cloud user want to store their data in the cloud environment in a secured way. To do this process user want to send the request to the cloud server to offer the security services.

STEP 2: After receiving the response from the server. The user can encrypt the original data using ECS cloud security algorithm and it will produce an encrypted data.

STEP 3: The cloud user can store their encrypted data in the cloud storage environment

STEP 4: Again the user can download the encrypted data from the cloud storage environment

STEP 5: The downloaded encrypted data is decrypted using the ECS cloud security algorithm and it will produces the original data

STEP 6: Finally, the user can get his original data in a safest manner from the cloud environment

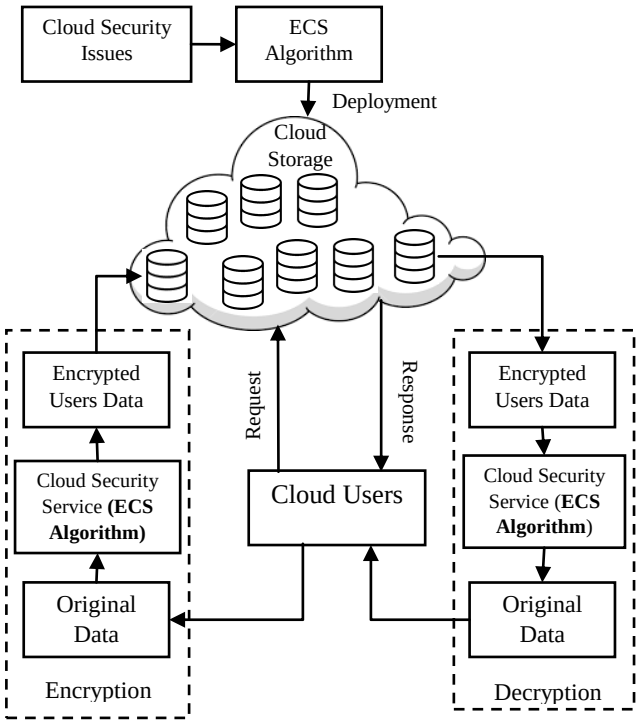

Fig 3. Proposed Methodology for Cloud Security

VIII. RESULT ANALYSIS

The proposed ECS algorithm was developed and deployed in the cloud environment. This ECS algorithm was tested using the Microsoft Azure Platform. In this platform different size of user data are given as input and the encryption and decryption times are taken for the proposed ECS Algorithm. The proposed algorithm was compared with various cryptographic algorithms.

The comparison results are tabulated in table 1 and it is graphically represented in figure 4.

TABLE 1. Comparative Analysis Based on Encryption & Decryption Time

Size	Algorithms			
	AES	Blowfish	RC6	ECS
	Encryption & Decryption Time(Seconds)			
5 MB	20.54	20.82	17.96	10.69
10 MB	22.81	21.68	18.74	15.96
15 MB	24.86	23.647	22.48	17.63
20 MB	29.54	25.48	24.79	20.75

Fig 4. Comparative Analysis based on Encryption and Decryption Time

The security level of the proposed ECS algorithm and the various security algorithms were computed in percentage. The result shows that AES is 75%, Blowfish is 79%, RC6 is 82% and ECS is 89% and the results are tabulated in table 2 and also it is graphically represented in figure 5. From the comparative analysis the proposed ECS algorithm shows better performance in the cloud environment.

TABLE 2: Comparative Analysis of The ECS And Existing Algorithms

Algorithms	Security Level(%)
AES	75
Blowfish	79
RC6	82
ECS	89

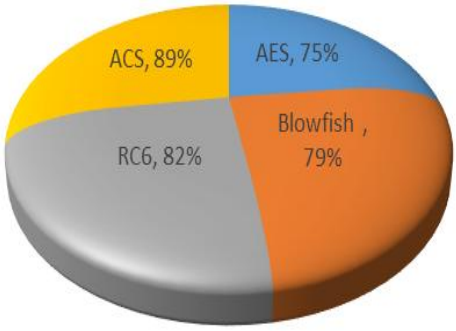

Fig 5. Comparative Analysis of the ECS and Existing Algorithms

IX. CONCLUSION

Cloud computing is an emerging technology that share the resources in the on demand manner over the internet. In this technology securing the users data is the biggest challenge task. The issue was overcome by developing the cloud security algorithm using various cryptographic techniques. In this research article a new cloud security algorithm was proposed using the cryptographic techniques in a hybrid manner. This algorithm was implemented and deployed in the cloud environment. The proposed algorithm was compared with various cloud security algorithms. The comparative result shows that the proposed algorithm shows better result. Hence the ECS algorithm provides better security for the user's data over the cloud environment.

REFERENCES

1. Ling Qian, Zhiguo Luo, Yujian Du, and Leitao Guo, "Cloud Computing: An Overview", Springer LNCS, 2009, pp. 626-631.
2. https://sites.google.com/site/cloudwikipedia/home/types-of-services/deployment-models-in-cloud-computing, Date:21/5/2019
3. R. Kowslaya, K.Subhashri, W.Rose Varuna,"Cloud Deployment Models, Benfits and Its Challenges", IOSR Journal of Engineering (IOSRJEN), 2018, PP. 48-53.
4. Bele, "An Empirical Study on Cloud Computing", International Journal of Computer Science and Mobile Computing, Volume 7, Issue.2, 2018, pp.33-41.
5. A Venkatesh, Marrynal S Eastaff, "A Study of Data Storage Security Issues in Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3, Issue 1,2018, pp.1741-1745.
6. https://www.wclghana.com/cloud-vs-on-premises-finding-the-right-balance/, Date:21/5/2019
7. Joseph Selvanayagam, Akash Singh, Joans Michael,Jaya Jeswani,"Secure File Storage on Cloud using Cryptography", International Research Journal of Engineering and Technology (IRJET), Volume: 05, Issue: 03,2018, pp. 2044-2047.
8. Ashima Narang, Deepali Gupta,"Different Encryption Algorithms In Cloud",International Journal of Engineering, Science and Mathematics, Vol. 7,Issue 4,2018, pp.429-432
9. Alkharji, Majedah & Liu, Hang. (2018). Homomorphic Encryption Algorithms and Schemes for Secure Computations in the Cloud.
10. Diksha Gupta, Partha Sarathi Chakraborty, Pragya Rajput, "Cloud Security Using Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2,2015, pp 425-429.
11. Gangolu Sreedevi, Prof. C. Rajendra," ICCC: Information Correctness to the Customers in Cloud Data Storage", June 2016, pp 321-326.
12. Nanda Hanamant Khanapur,Arun Patro,"Design and Implementation of Enhanced version of MRC6 algorithm for data security", International Journal of Advanced Computer Research, Volume-5, Issue-19, 2015, pp. 225-232
13. N.A. El-Fishawy, T.E. El-Danaf, O.M. Abou Zaid,"A modification of RC6/sup tm/ block cipher algorithm for data security (MRC6)", International Conference on Electrical, Electronic and Computer Engineering,2014,pp.222-228
14. Ajay Bhushan, Pawitar Dulari, "TORDES-The New Symmetric Key Algorithm", Journal of university of anbar for pure science, Volume 6, Number 2, 2012.

AUTHORS PROFILE

Dr. J. Charles Selvaraj is working as Associate Professor & Head, Department of Computer Science, Arignar Anna Govt. Arts College, Musiri. He has 22 years of experience in teaching and 10 years of experience in research. He has published more than 20 research articles in the International / National Conferences and Journals. His research interests are Software Engineering, Cognitive Aspects in Programming, and Cloud Computing.

Dr. V. Arul Kumar is working as Assistant Professor in School of Computer Science & Applications, REVA University. He completed his doctoral degree in Computer Science from Bharathidasan University-Tamil Nadu. He has completed M.Phil in Computer Science from Bharadhidasan University, Tamil Nadu. He has 7 years of experience in research. He has published more than 25 research articles in the various International / National Journals and conferences. His research area includes data Mining, cloud security, and cryptography.

Francis Densil Raj V is presently working as Assistant Professor in REVA University, Bangalore, India. His thirst area of Research spreads towards Networks and IoT. He is having more than 5 publications in indexed journals. Now he is working with Routing Algorithms in IoT.

Dr. A. DalvinVinoth Kumar is working as Assistant Professor in the Department of Computer Science, Kristu Jayanthi College Bengaluru, Karnataka, India. His research interests are: MANET, Routing and IoT.