IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Multi Security Algorithm Based Security Model to Achieve Confidentiality & Apply Authentication in Cloud Environment: A Survey

Arpit Agrawal[1*], Ankit Singh Yadav[2]

[1,2]Computer Engineering, Institute of Engineering & Technology (IET), DAVV, Indore, India

Corresponding Author: aagrawal@ietdavv.edu.in, Tel.: +91-94240-90249

DOI: https://doi.org/10.26438/ijcse/v7i6.10511054 | Available online at: www.ijcseonline.org

Accepted: 11/Jun/2019, Published: 30/Jun/2019

***Abstract*—** Due to the sharing of distributed resources through an insecure network in an open environment, cloud faces security issues therefore easy access of data is possible from anywhere. Also due to many reasons security and privacy, issue arises at the same time. Increasing demand of resources and development of new technology are the reason for the open and shared data storage. Therefore, this condition needs the secure data storage services in cloud environment. In the public cloud environment, the service provider is not the trusted provider. Different security issues for data in cloud environment is proposed in this paper with some methods for security services such as confidentiality, authorization and authentication.

***Keywords*—**Cloud Computing, Security, ECC, BLOWFISH

I. INTRODUCTION

Clouds model are integrated with various technologies like web services, virtualization, and for management of applications service level agreement are used (SLA). Many customers service providers are turned towards cloud environment because of rapid growth in technologies. For the network connectivity, different cloud services are used by the military, commercial system and government to get the availability of high services to the user. The future of IT sector is visualized in cloud computing. Cloud computing is the integrated form of virtualization and automation. It aims as differentiating operating system from the hardware. It provides pay as peruse service, which is scalable. Services can be easily accessible in cloud by anyone. It is not completely secure because of its open nature but needs to be secure for the security purpose. Private cloud is owned and used by an organizations with limited services and limited accessibility to system and is limited to a particular organization. Due to its private nature, it is more secure than public cloud. Hybrid cloud is the combination of public and private cloud; public cloud performs non-critical activities and in private cloud performs critical activities. Advantages for secure applications are taken by organizations for the deployment model on private cloud. For the cost benefit, applications data are shared. Community cloud is like a private cloud in which group of organizations are serve with the services.

A. Cloud Computing

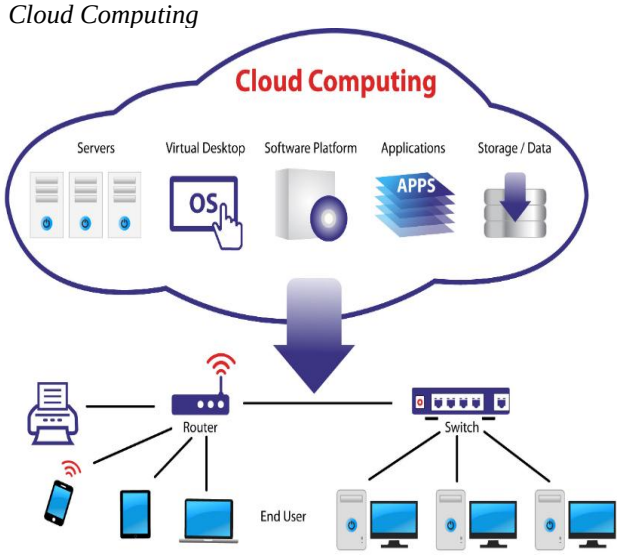

Figure 1. Cloud Computing

Cloud computing is the shared pool of resources which is open and is vulnerable. It is popular because of its wide use and massive storage. In cloud, data can be stored and retrieved. User can use its services and access resources. Technology servers their customers with different services with providing secure data. Cloud computing is also a data center, a cloud data center. Here, sharing and storing of data can be possible by user from anywhere at any time but with the availability of internet. Large data emerges from many websites and these data is to be stored somewhere at

particular place, these websites carrying a bulk data are e-commerce websites, social networking sites and also arrangement of these data are very important. Over an internet, users are serving with the on demand services. Service like deploying, storing, configuring and sharing can be achieved. Large data of networking sites, emails etc. are stored in cloud.

B. Cloud security can be achieved using following terms:

1. Data Security: The identity access management can achieve Data security, risks of multi tenancy, availability and backup, data privacy and security.
2. Physical Security: Data location, server, storage and network are calculated in physical security.
3. Organizational: Organization with resource planning, change management and malicious insider, which is important to detect.
4. Technological: Application development, portability, lack of interoperability standards is essential in technological security.
5. Compliance & Audit: Compliance and audit consisting of legal challenges, business continuity and disaster recovery.

Organization of paper follow in such a way that, Section I consist Introduction for the topic on which work is proceeding. Section II contains related work on which research has been done previously by authors. Section III contain the problem of the work on which the proposed work is established, Section IV contain methodology of the work. Section V concludes conclusion and future implementation of research.

II. RELATED WORK

Algorithmic approach is described in this related work with the techniques and mitigation approaches for basic improvement.

Bih-Hwang Lee [1] proposed a possible method to encrypt data is Advanced Encryption Standard (AES). Similar to cloud computing, Heroku was implemented by author in the proposed work. Some of the highlights of this work is as:

- For implementation of data security in Heroku, author used AES algorithm.
- AES is used for data security as a cryptographic algorithm
- Calculation of delay time in encryption shows large data size with increased delay time.

Cloud computing [2] illustrates different attributes, which are elaborated below:

1. Self-requisite of resources: Requirement includes processing capabilities, storage, software and other provision for network services.
2. Shared Resources: It includes corporate models for which shares resources, multiple users in same network shares resources at different levels like application, host and network level.
3. Scalability: Scalability is the ability to manage thousands of systems, storage and manage large bandwidth.
4. Resistance: Promptly escalation and reduction of resources as per user requirement.
5. Pay-per-use: It is cost effective in term where, use have to pay for the used resource.

Deyan Chen et al. [1] described about security in cloud and research about it with its drawbacks. Cloud security applications are designed and its significance are analyzed and discussed in multiple dimensions. This approach suggests that the technology is not completely adopted till now. The advantages and disadvantages of cloud security, its complete architecture is discussed.

Vishwanath S Mahalle et al. [2] performs the security measures with the use of three keys. Logic of this says that if one key compromise then the other key will not permit user maintain the security by using three keys, the logic behind the work is that even if one key will be comprised the other two key will not allow the user to get into the system. In this work, the security is applied at administrator end as well in order to have secure transaction.

Chang et al. [3] proposed about the platform for financial software as a service (SaaS) and about security framework in cloud. He demonstrated that the financial services on cloud can be achieved by the following features like scalability, flexibility, reliability, security, accuracy, speed and probability. The author mainly concluded about the financial service on cloud and how it can be achieved using SaaS or framework.

III. PROBLEM DOMAIN

Problem faced in the proposed work is security issue. This type of issue arises due to the open nature of cloud where there is easy to access any data. In public cloud environment, anyone from anywhere can access resources and use service on demand. The data access in is the form of plain text, which can be easily accessed.

The proposed approach used in our work is for protecting the private data. Data protection is essential for the purpose of authentication. If any user "A" stores his data in cloud and another user "B" want to access that data for any malicious activity then the data of user "A" should be secured, so that no one can access it. In most of the research homomorphic encryptions are used on the data mining approach to encrypt the data but for the better security, we have used hybrid approach in our paper.

IV. PROPOSED METHODOLOGY

Methodology says that proposed model ensures security by encrypting data automatically with using vigorous algorithm that gives accurate and fast result. Methodology includes MD5 to achieve integrity, ECC to achieve authentication and Blowfish to achieve confidentiality. The complete encryption process has been shown in below figure.

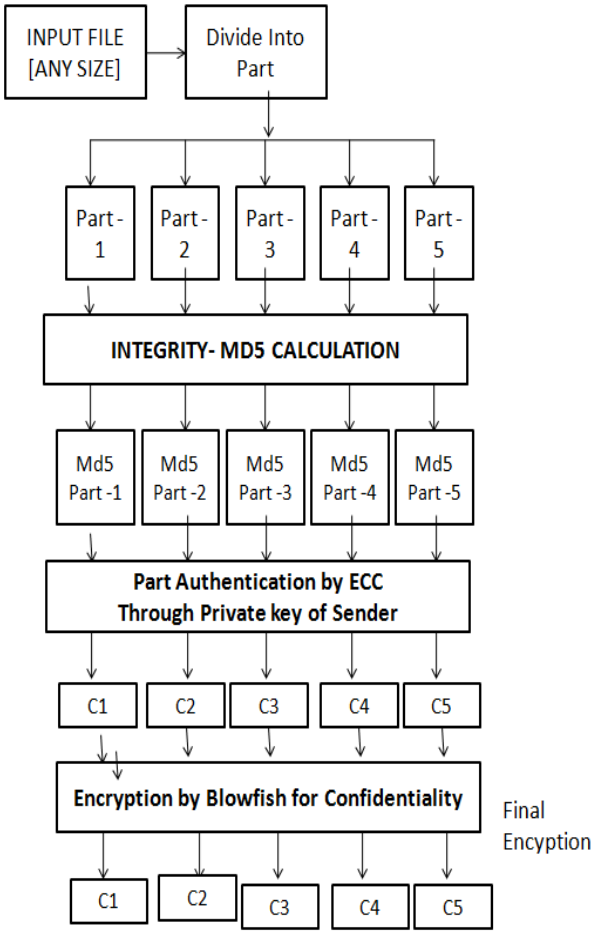

Figure 2. Encryption Process

Encryption process helps us to implement data privacy and keep data confidentiality safe.

The complete decryption process is shown in figure 2. Encryption and Decryption process is performed using different algorithms. Integrity is calculated using MD5, Authentication using ECC and Confidentiality using Blowfish. Similar steps will be performed for decryption.

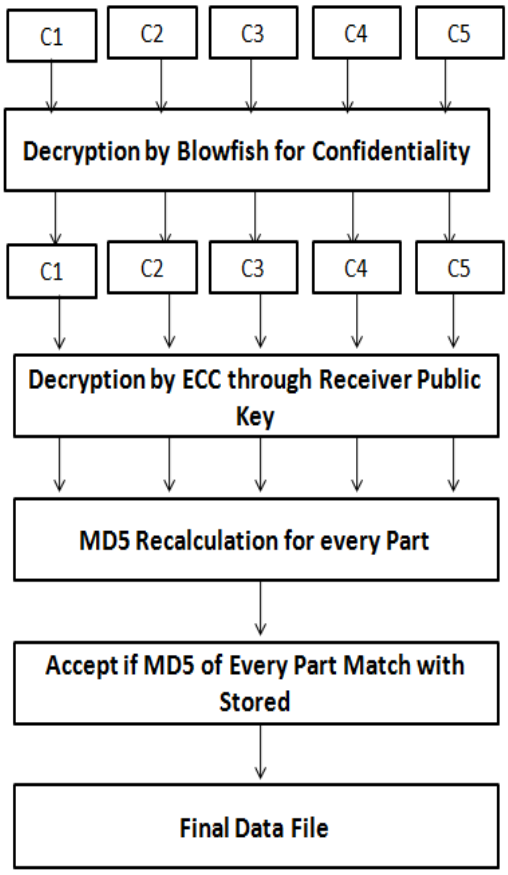

Figure 3. Decryption Process

V. CONCLUSION AND FUTURE SCOPE

Presented work focuses on security of data in cloud using different encryption and decryption algorithms. In addition, the security services like authentication, authorization, confidentiality and integrity is required to accomplish for proper accuracy. This mechanism of using encryption and decryption algorithm with security service leads to genuine flow of architecture. The article proposed solution using ECC and Blowfish and are combined to form hybrid approach to achieve authentication. No other user can access data of another user of cloud with detecting suspicious activity in cloud.

REFERENCES

[1] Bih-Hwang Lee, Ervin Kusuma Dewi, "*Data Security in Cloud Computing Using AES under HEROKU Cloud*". **27th** Wireless and Optical Communications Conference, IEEE (WOCC2018), **2018**.

[2] L. Foster, Y. Zhao, I. Raicu, S.Y. Lu, "*Cloud computing and grid computing"* 360-degree compared, in: Grid Computing Environments Workshop, GCE'08, Austin, TX, Nov. **12-16, 2008**, pp. **1-10**.

[3] J.W. Rittinghouse, J.F. Ransome, "*Cloud Computing Implementation, Management, and Security*". CRC Press, Boca Raton, **2009.**

[4] Deyan Chen; Hong Zhao, "*Data Security and Privacy Protection Issues in Cloud Computing*," in Computer Science and Electronics Engineering (ICCSEE), **2012** International Conference on , vol.1, no., pp.**647-651, 23-25 March 2012.**

[5] Vishwanath s Mahalle, Aniket K Shahade, *"Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm".* Power, Automation and communication (INAP), **2014.**

[6] V. Chang, C.-S. Li, D. De Roure, G. Wills, R.J. Walters, and C. Chee, *"The financial clouds review".* Cloud Computing Advancements in Design, Implementation, and Technologies, vol. **125, 2012**.

[7] A. Lopez-Alt, E. Tromer, and V. Vaikuntanathan, *"On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption",* in Proceedings of the forty-fourth annual ACM symposium on Theory of computing. ACM, **2012,** pp. **1219-1234**.

[8] M. Brenner, J. Wiebelitz, G. Von Voigt, and M. Smith, *"Secret program execution in the cloud applying homomorphic encryption",* in 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011). IEEE,**2011**, PP.**114-119.**

Authors Profile

Mr. Arpit Agrawal pursed Bachelor of Science from DAVV University, India in 2006 and Master of Science from DAVV University in year 2011. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Engineering, India since 2006. He has published more than 10 research papers in UGC approved and it's also available online. His main research work focuses on Natural Language Processing, Information Security, Big Data Analytics, and Data Mining. He has 13 years of teaching experience and 5 years of Research Experience.

Mr Ankit Singh Yadav pursed Bachelor of Engineering from RGPV University, India in 2013. He is currently pursuing Master of Science from DAVV University, India. His research interest are in different security concept especially in cloud security and confidentiality.

