Research Article

ACCENTS Transactions on Information Security, Vol 4(13)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2018.312001

An efficient method for cloud computing security and sharing in private cloud environment

Mahale Rahul bhaskar[1*], Kailash Patidar[2], Rishi Kushwah[3] and Sudeesh Chouhan[3]
M.Tech Scholar, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[1]
Professor and HOD, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[2]
Assistant Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[3]

Abstract

In this paper an efficient approach for private cloud data security has been maintained by the advanced encryption standard (AES) with additional XOR and RC6 key variant mechanism. The benefit of AES is robust and provides the variability in higher key length sizes. So the combination is highly secure. In addition to this we have shuffle the data again with the additional XOR mechanism which will provide more security. This shuffled data is process with the RC6 key variant mechanism. The hybridization provides the higher key variability along with the key variant mechanism in all the iterations so the key combinations changed in all the iteration and for the same data. Our approach also provides the security breach indication in terms of data breach attack when the data is transferred through cloud computing environment.

Keywords

Cloud computing, AES with XOR, RC6, Private cloud.

1.Introduction

In the current business arena cloud computing is very helpful and cost effective for small business as well as for the larger business [1−5].

In the today's world the use of cloud computing is spreading in different areas. It includes the university, business enterprise, IT industry, Health sector etc. The security concern is the major concern these days. There are several literature which discussed this type of issues like [6−10]. Virtualization, dominating enlisting is additionally the more obvious office parts of passed on preparing. In any case, to satisfy the execution on the parallel framework and keeping up the decency is convincing [11]. In every single one of these works, stunning attempts are made to plan strategies that meet assorted fundamentals: high game plan feasibility, stateless check, unbounded use of request and wretchedness of information, and so forth.

Thinking about the piece of the verifier in the model, every last one of the plans showed before fall into two classes: private auditability and open auditability [5]. Despite the manner in which that orchestrates with private auditability can play out the plans enough, yet it is attempting circumstance if the information is anchoring quietly [5]. Virtualization is the key fragments of scattered figuring by which information sharing is conceivable between various machines of virtual closeness from the server develop [12, 13]. Virtualization draws in the live relocation [9] of virtual machines which helps in keeping up the guaranteed SLA to the cloud client other than to change stack crosswise over physical servers in the information centers [12].

In the cloud provider market the main providers are Google, Microsoft, Amazon and Salesforce.com. The appropriated figuring advantage show relies upon the data correspondence layer. The whole correspondence is relies upon three layers. The layers of the cloud computing are: Software as a Service (SaaS) which is for the software based application.

*Author for correspondence

Customer relationship organization (CRM) is the example [14]. Platform as a Service (PaaS) is fior the platform based application for he different deployment services. Infrastructure as a Service (IaaS) by and large joins virtualization conditions as got associations rather than physical or submitted PC gear [15].

The main objectives of this paper are:

1. To apply standard encryption and decryption mechanism with security breach detection.
2. To perform analytical and comparative study.

2.Literature survey

In 2017, Akhil et al. [16] discussed the data security in the cloud environment as the number of users in the cloud is large. They have focus on the data security aspects when the data is secured. They have suggested that the intruders can act as the third party and can gain the access. So they have suggested encryption technique for the data security. Their results show that the approach can enhance the security system.

In 2018, Alsaidi and Kausar [17] suggested that internet of things (IoT) plays an important role in the human life. They have focused on the security threats in different areas of IoT technology. They have also presented the cloud architecture associated with IoT with different area of application like smart cities, telemedicine and intelligent transportation system.

In 2018, Elliott et al. [18] suggested the use and applicability of different containers and containerizing services. They have presented a novel approach for the container management. It is helpful in the case of private, public, or hybrid clouds. For improving the security aspects they have

In 2018, Elsayed and Zulkernine [19] suggested the linking and innovation through cloud computing with the big data. They have suggested the security threats that can be the risk for the big data are analytic applications that are malicious and vulnerable. They have presented real-time security monitoring as a service (SMaaS). Their focus is the detection of the security anomalies for the Hadoop clusters. Their focus is to detect the vulnerability which can breach the data integrity and confidentiality. They have also maintained the information flow in terms of log data. They have also evaluated their performances.

In 2018, Feng et al. [20] suggested insurer for the cyber risk insurance. It provides the insurance like any other insurance but it covers the damage of the cyber threats. They have investigated the pricing for the cloud-insurance market. It includes the users, cloud providers, and cloud-insurers.

In 2018, Gordin et al. [21] suggested the use for the companies to take the benefits of Google cloud, Amazon EC2 and Microsoft Azure. They have suggested that in case of public clouds in general providers assure the security. In case of private clouds it is a concern of research as the security may maintain by third party so the vulnerability may arise. They have performed the study for the private cloud solution. They have also experimented and check the hypervisor-based virtual machines isolation.

In 2018, Halgaonkar et al. [22] suggested security issues in case of vehicular adhoc network (VANET). They have discussed VANET in terms of cloud computing. They have discussed the advantages of road side unit (RSU). But they have suggested the cost & security as the main disadvantages. They have provided the direct communication approach for reducing the cost and enhancing the security.

In 2018, Lee et al. [23] suggested the need of network security in case of cloud computing. They have suggested that cloud platform utilizes third-party data centers model like in case of PaaS is Heroku. Heroku supports different programming languages. They have suggested security issues which can be handle by advanced encryption standard (AES). They have implemented AES for data security in Heroku. Their result support the AES standard for the security.

In 2018, Li and An [24] discussed the need of cloud storage and security. They have suggested that the security concern is very important concern now a days in case of cloud computing. They have focused on improvement of policy storage and the improvement of clod security issues.

In 2018, Nguyen et al. [25] discusses the increasing demand of the campus cloud infrastructures. They have also focused on dealing with the very strict policy on the security requirements. But they have suggested that campus private clouds (CPC) are not fully secure.

So they have proposed a cost-effective, and moving target defense (MTD) based cloud resource adaptation approach. They have proposed a Bayesian attack graph (BAG). It is proposed as the threat assessment model. They have followed the protocol of common vulnerability scoring system (CVSS). They have evaluated on the city university of New York (CUNY) research network. The examination includes one of kind situations with various privacy, honesty, and accessibility related vulnerabilities being abused by assaults from various system areas. At last, we reproduce a CUNY inquire about system in condition to approve our Sack display by imitating assault situations and watching framework versatility with and without MTD.

In 2018, Paikrao and Patil [26] suggested that the resources sharing and economical computing is the main concern in cloud computing. But due to the resource sharing approach there are several security concerns. They have considered and classify them comprehensively like issues recognized by CSA, issues distinguished because of area of the information, issues acquired from systems administration and all the more significantly the issues brought because of vulnerabilities up in virtualization. Hypervisor vulnerabilities are zone of worry similarly as VM the board is concerned. A security as an administration is proposed for virtualization vulnerabilities.

In 2018, Souaf et al. [27] suggested that there is a race for providing better cloud services by different cloud providers. So the adequate provider selection becomes a challenge now days. They have proposed a brokerage solution for the security properties in case of inter-VM relations. Their method used the finite model finder KodKod for the consistency verification for the deployment model.

3.Proposed method

This framework has been designed and developed on Java environment with the help of NETBEANS IDE. The pages have been developed by the help of Java Server pages (JSP). The servers are created based on APACHE Tomcat server. For the method exploration four servers have been created as the cloud providers as well as for the resource sharing. The servers have different storage virtualization with different specializations also so that it can help in data virtualization mechanism and also supports the other resources. Although the cloud users can choose any servers with different requirement capacity for the use of data and resources in the same sort of data series. *Figure 1* shows the block diagram of the approach. The data is loaded with the communication load variants which is unique for the one communication and it will be notified as soon as any unauthenticated communication may happens.

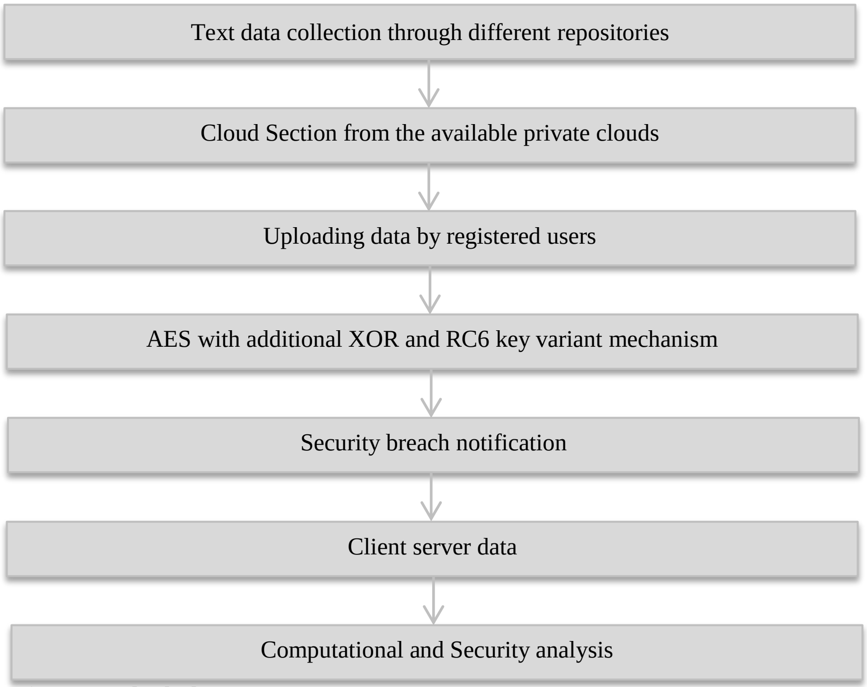
Text data collection through different repositories
Cloud Section from the available private clouds
Uploading data by registered users
AES with additional XOR and RC6 key variant mechanism
Security breach notification
Client server data
Computational and Security analysis

Figure 1 Block diagram

4.Results

Figure 2 shows the comparison based on the property in the traditional and proposed mechanism. *Figure 3* shows the average time calculated for cryptography by pevious algorithm analyses. The results clearly indicates that our approach has the capability to improves the cloud user security.

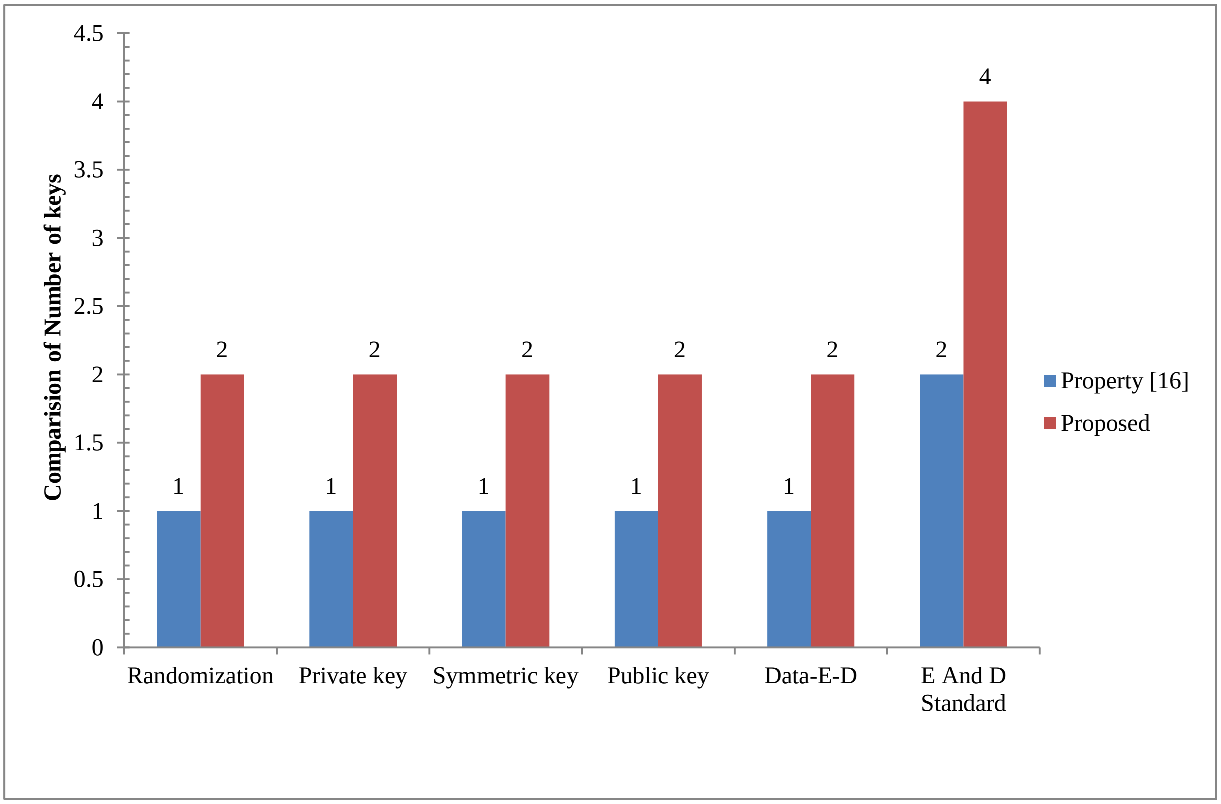

Figure 2 Security analysis

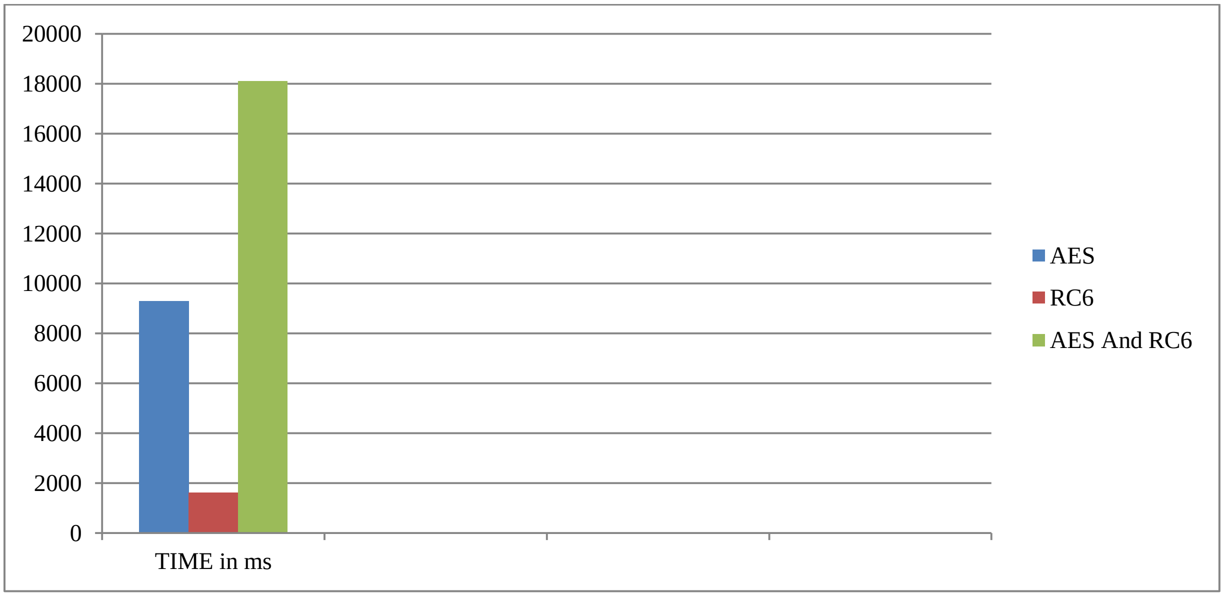

Figure 3 Average time calculated for cryptography by various algorithm analysis

5.Conclusion

In this paper an efficient private cloud security mechanism have been demonstrated for the data security by the help of AES with additional XOR and RC6 key variant mechanism. It provides the communication based on inter and intra cloud environment as well as data sharing mechanism with on demand cloud virtualization. The sever pages have been developed based on the java server pages and server local host support has been provided by APACHE Tomcat server. The main benefit of this approach is the hybrid standard security for the data in times of communication another advantage is the communication load which is helpful in the identification of data breach or security alert in case of unauthorized access. The results supports the advantages of our approach.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, et al. Above the clouds: a berkeley view of cloud computing. Department of electrical engineering and computer sciences, university of california, Berkeley, Rep. UCB/EECS. 2009; 28(13):2009.

[2] Ruiz-Agundez I, Penya YK, Bringas PG. Cloud computing services accounting. International Journal of Advanced Computer Research. 2012; 2(4):7-17.

[3] Singh A, Shrivastava M. Overview of security issues in cloud computing. International Journal of Advanced Computer Research. 2012; 2(1):41-5.

[4] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, et al. Provable data possession at untrusted stores. In proceedings of the conference on computer and communications security 2007 (pp. 598-609). ACM.

[5] Seng LK, Ithnin N, Said SZM. The approaches to quantify web application security scanners quality: a review. International Journal of Advanced Computer Research. 2018; 8(38): 285-312.

[6] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI international conference on software engineering 2012 (pp. 1-8). IEEE.

[7] Malathi M. Cloud computing issues-a survey. International Journal of Advanced Computer Research. 2012;2(4):113-18.

[8] Nagar N, Jatav PK. A secure authenticate framework for cloud computing environment. International Journal of Advanced Computer Research. 2014; 4(14):266-271.

[9] Adebisi AA, Adekanmi AA, Oluwatobi AE. A study of cloud computing in the university enterprise. International Journal of Advanced Computer Research. 2014; 4(15):450-8.

[10] Tsai WT, Sun X, Balasooriya J. Service-oriented cloud computing architecture. In seventh international conference on information technology: new generations 2010 (pp. 684-9). IEEE.

[11] Patra GK, Chakraborty N. Securing cloud infrastructure for high performance scientific computations using cryptographic techniques. International Journal of Advanced Computer Research (IJACR). 2014; 4(1):66-72.

[12] Sikarwar C, Patidar K, Kushwah R. K-means and associated cuckoo based hierarchy optimization for document categorization. International Journal of Advanced Technology and Engineering Exploration. 2018; 5(45): 297-302.

[13] Zheng L, Hu Y, Yang C. Design and research on private cloud computing architecture to support smart grid. In third international conference on intelligent human-machine systems and cybernetics 2011 (pp. 159-61). IEEE.

[14] Hay B, Nance K, Bishop M. Storm clouds rising: security challenges for IaaS cloud computing. In international conference on system sciences 2011 (pp. 1-7). IEEE.

[15] Ogigau-Neamtiu F. Cloud computing security issues. Journal of Defense Resources Management. 2012; 3(2):141.

[16] Akhil KM, Kumar MP, Pushpa BR. Enhanced cloud data security using AES algorithm. In intelligent computing and control (I2C2), international conference on 2017 (pp. 1-5). IEEE.

[17] Alsaidi A, Kausar F. Security attacks and countermeasures on cloud assisted IoT applications. In international conference on smart cloud (SmartCloud) 2018 (pp. 213-17). IEEE.

[18] Elliott D, Otero C, Ridley M, Merino X. A cloud-agnostic container orchestrator for improving interoperability. In 11th international conference on cloud computing (CLOUD) 2018 (pp. 958-61). IEEE.

[19] Elsayed M, Zulkernine M. Towards security monitoring for cloud analytic applications. In 4th international conference on big data security on cloud (BigDataSecurity), IEEE international conference on high performance and smart computing,(HPSC) and IEEE international conference on intelligent data and security (IDS) 2018 (pp. 69-78). IEEE.

[20] Feng S, Xiong Z, Niyato D, Wang P, Wang SS. Joint pricing and security investment for cloud-insurance: a security interdependency perspective. In wireless communications and networking conference (WCNC), 2018 (pp. 1-6). IEEE.

[21] Gordin I, Graur A, Potorac A, Balan D. Security assessment of OpenStack cloud using outside and inside software tools. In international conference on development and application systems (DAS) 2018 (pp. 170-4). IEEE.

[22] Halgaonkar PS, Kathole AB, Nadaf JS, Tambe KP. Providing security in vehicular Adhoc network using cloud computing by secure key method. In international conference on information, communication, engineering and technology (ICICET) 2018 (pp. 1-3). IEEE.

[23] Lee BH, Dewi EK, Wajdi MF. Data security in cloud computing using AES under HEROKU cloud. In wireless and optical communication conference (WOCC), 2018 (pp. 1-5). IEEE.

[24] Li L, An X. Research on storage mechanism of cloud security policy. In international conference on virtual reality and intelligent systems (ICVRIS) 2018 (pp. 130-3). IEEE.

[25] Nguyen M, Samanta P, Debroy S. Analyzing moving target defense for resilient campus private cloud. In 11th international conference on cloud computing (CLOUD) 2018 (pp. 114-21). IEEE.

[26] Paikrao RL, Patil VH. Security as a service model for virtualization vulnerabilities in cloud computing. In international conference on advances in communication and computing technology (ICACCT) 2018 (pp. 559-62). IEEE.

[27] Souaf S, Berthome P, Loulergue F. A cloud brokerage solution: formal methods meet security in cloud federations. In international conference on high performance computing & simulation (HPCS) 2018 (pp. 691-9). IEEE.