International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 22 (2017) pp. 12982-12988

Encryption as a Service Based on Parallelizing Fully Homomorphic Encryption Implementation on Openstack Cloud Computing

Ouadia Zibouh[#1], Anouar Dalli [*2] and Hilal Drissi [#3]
[1,3] *Systems Analysis, Information Processing and Integrated Management Laboratory*
Superior School of technology-Sale, Mohammed V University in Rabat, Morocco.
29,Rue Sénégal Etage 1 Apt 3 Océan Rabat Morocco.
[2] *Telecommunications and Networks Engineering Department, National School of Applied Sciences-Safi,*
Cadi Ayyad University in Marrakesh, Morocco, Route Sidi Bouzid BP 63, 46000 - Safi, Morocco.

Orcid : [1]0000-0001-9420-5274, [2]0000-0002-5216-4248

Abstract

Cloud computing nowadays is a fundamental change happening in the area of Information Technology. It plays a crucial role in terms of data storing and reducing the overall cost to entrepreneurs. However, data security continues to be one of the top concerns for cloud computing. To provide the secure data storage and retrieval, many techniques have been proposed but the majority of them face some drawbacks which diminish the functionality of Cloud Computing. The biggest and most important benefit that gains private cloud, where an organization sets up an internal cloud infrastructure, is security advantages which can lead to lower costs and improved performance. The most common open source of cloud frameworks that allows the customers to build their own private IaaS (Infrastructure as a Service) cloud are OpenStack, Eucalyptus and OpenNebula. This paper provides a comparative study of these three cloud middlewares. This work scrutinizes the Fully Homomorphic encryption which allows performing operations on encrypted data without compromising the encryption. The main aim of this paper is to propose a new architecture to secure cloud computing, prevent security risks and improve the performance and the time of data processing. This framework is based on Cryptography as a Service (CaaS) including the private cloud OpenStack platform.

Keywords: Cloud Computing, Security, Fully Homomorphic encryption, OpenStack, Eucalyptus, OpenNebula.

INTRODUCTION

Today**,** most of the large and small-scale businesses are increasingly turning to the cloud computing for better business IT solutions. Its scalable and elastic resources will reduce the customer cost. However, outsource the data, the application or the whole virtual machines outside the customer security parameter raises new security challenges. Security remains a key decision factor for migration of resources to the cloud. The cloud is a multi-tenant environment and both the provider and tenant have more security threats [1]. Security ensures the encryption of the data before sending it to the cloud. But actually performing computations on that data stored in the cloud requires decrypting it first. This makes sensitive and critical data available to the cloud provider. The proposal here is to encrypt data before sending to the cloud providers using a cryptosystems based on Homomorphic Encryption which allows performing computations on encrypted data without decrypting. This technique avoids the problem of providing the encryption key to the cloud provider in order to perform the calculations required. Users of IaaS can control and manage their virtualized infrastructure resources. However, using an external IaaS provider can contribute to relatively high costs, and may not be appropriate for many enterprises or organizations and their applications. Therefore, implementing their own cloud for these enterprises or organizations requires a reliable and elastic open source management platform tool, which has devoted a great attention in this area [2]. The use of open source cloud frameworks has been recently increased. OpenStack, Eucalyptus and OpenNebula are the most widespread open source cloud frameworks that allow the customers to build their own private IaaS (Infrastructure as a Service) cloud. OpenStack has become the largest project in open source cloud framework solution for building private and public clouds within some of the biggest IT companies in the world-over 180 companies contributing and more than 6,000 individual members in 76 countries[3].

The rest of the paper is organized in the following sections. Section II presents theoretical background and the basic concepts of the homomorphic encryption. Section III scrutinizes the comparisons of open source IaaS cloud management platforms covered in this review: OpenNebula, Eucalyptus and OpenStack .In Section IV, we briefly describe the Openstack cloud architecture and its components. Section V describes the proposed approach to decrease cloud security risks and improve the performance of processing done on sensitive data users. Finally, the conclusion put all the study in a nutshell and presents future work.

HOMOMORPHIC ENCRYPTION

Homomorphic encryption technique applied on the cloud computing security is expected to play an important part in cloud computing, allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider's analytic services. Using this technique, operations can be applied on encrypted data without compromising the encryption. Once operations are performed on client data by the cloud provider, the client can decrypt the result achieving its goal without the cloud provider server knowing anything about the data it operated on and the client is the only holder of the secret key. The decryption of the result of any operation provides the same result as if we have worked directly on the plain text data.

The idea of homomorphic encryption was suggested for the first time by Rivest, Adlemanand Dertouzos in 1978[4]. They used in their suggestion some restricted classes of functions such as addition or multiplication. Since then, little progress has been made for 30 years. In 1982, Shafi Goldwasser and Silvio Micali[5] proposed their encryption system that helps to encrypt one bit in additive homomorphic encryption. In the same concept in 1999, Pascal Paillier[6]was also proposed a provable security encryption system that was also an additive Homomorphic encryption. In 2005, Dan Boneh, Eu-Jin Goh and Kobi[7] invented a security system of encryption that can do one multiplication and unlimited number of additions .In 2009 [8], Craig Gentry constructs, for the first time, a fully homomorphic encryption(FHE) that could (inefficiently) do an arbitrary number of additions and multiplications in the same time. However, his system was very complex. Zvika Brakerski and Vinod Vaikunt anathan gave a simpler and also efficient FHE[9]. A number of Homomorphic cryptosystems have been proposed and the construction of secure and efficient systems is an active area of research especially given the popularity and dominance of cloud computing.

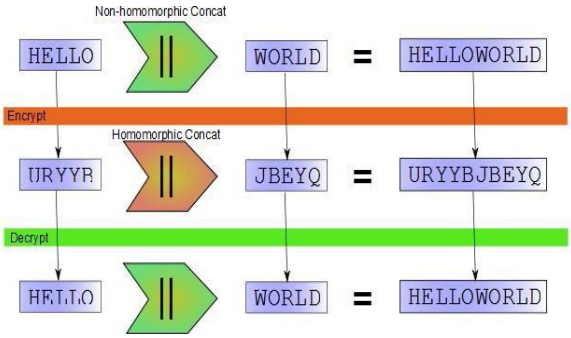

Figure 1: A string concat example of Homomorphic Encryption[10]

Homomorphic Encryption systems can be classified into different types based on the operations that they allow on their raw data. There are two main categories of homomorphic encryption schemes: Partially Homomorphic Encryption (PHE) and Fully Homomorphic Encryption (FHE) schemes.

A. Partially Homomorphic Encryption Systems

Partially homomorphic encryption systems allow performing only a single operation on encrypted data. Different types of partially homomorphic Encryption systems are as follows:

✓ Additive Homomorphic Encryption Systems

A Homomorphic Encryption is additive if it supports additive operations on encrypted data without the decryption of individual data's, it means that it can calculate Enc(x + y) from Enc(x) and Enc (y) without knowing x and y: Enc (x ⊗ y) = Enc(x) + Enc(y)

Example: Paillier Cryptosystem[9], Goldwasser-Micali Cryptosystem[11]

✓ Multiplicative Homomorphic Encryption Systems

A Homomorphic Encryption is multiplicative if it allows homomorphic computation of only the multiplication operation. Put differently, that it can calculate Enc(x × y) from Enc (x) and Enc (y) without knowing x and y:

Enc (x.y) = Enc(x).Enc(y)

Examples : RSA algorithm[12] and El Gamal encryption system[4]

✓ Additive and Multiplicative Homomorphic Encryption Systems

These systems allow arbitrarily many homomorphic computations of one type and limited number of operations of the other type. it allows both addition and multiplication operations but it is not fully homomorphic. An example of this kind would be Boneh-Goh-Nissim cryptosystem which supports performing unlimited number of addition operation but only one multiplication.

Example: Boneh-Goh-Nissim scheme[7]

B Fully Homomorphic Encryption Systems

Fully homomorphic encryption systems allow arbitrary number of additions and multiplications and thus calculate any types of functions on the encrypted data that is stored in the cloud without the need for any decryption. The constructing of this scheme has remained a central open problem in cryptography for more than 30 years and thought to be impossible until 2009, when Craig Gentry proposed the first plausible construction of a fully homomorphic scheme[5]. The application of this encryption is an important stone in Cloud Computing security. This means that operations on confidential data can now be outsourced to the cloud server keeping the secret key that can decrypt the result of the calculation.

The security issues of data stored in cloud can be solved by using Fully Homomorphic Encryption (FHE) schemes. To secure it, the data should be encrypted with FHE before sending it to the cloud. When the user wants the server to execute some processing on these encrypted data such as search, he can send encrypted request to the cloud server. The server performs the required operations without decrypting and sends the encrypted result to the user. Finally the user decrypts the data with his secret key to retrieve the correct result. Figure 2 clearly shows the work flow in FHE scheme which is used to protect the data to be encrypted. This technique avoids the problem to provide the encryption key to the cloud provider in order to perform the calculations required.

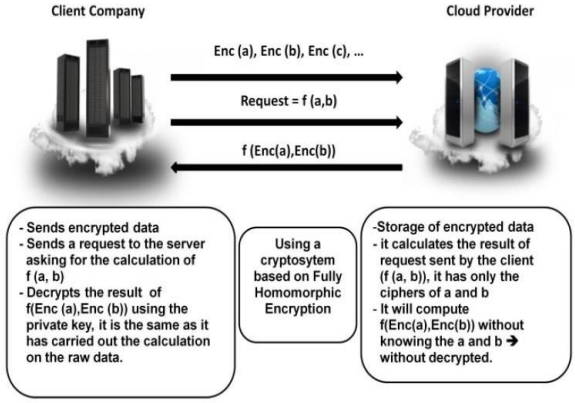

Figure 2: A Fully Homomorphic Encryption Implementation on Cloud Computing

COMPARATIVE STUDY OF OPEN SOURCE CLOUD SOLUTIONS

To deploy public or private cloud, there are many open source software available such as Eucalyptus, OpenStack and Open Nebula. We propose a comparative study of the three solutions in order to select the most appropriate solution to our criteria. The comparative study is based on the investigation of the architecture of respective open source platform.

- Eucalyptus is an open source private cloud software for building private or hybrid cloud. It enables pooling compute, storage, and network resources that can be dynamically scaled up or down as application workloads change. It is open source software which is compatible with Amazon Web Service (AWS) APIs. It was developed by University of California-Santa Barbara for Cloud Computing to implement Infrastructure as a Service (IaaS)[13]. It is coded in Java, Python and C languages with a central storage controller walrus and controllers on each node [14]. Eucalyptus supports many virtualization technologies such as KVM, VMware, Xen, and has been integrated into multiple varieties of Linux, and provides API to this layer which makes it look similar to EC2 [2]. Eucalyptus provides an Elastic Compute Cloud (EC2) -compatible cloud Computing Platform and Simple Storage Service (S3)-compatible Cloud Storage. Eucalyptus is comprised of some high-level components such as Cloud Controller (CLC), Cluster Controller (CC), Storage Controller (SC), and Node Controller (NC) [13].

- OpenNebula is another open-source cloud solution, subject to the requirements of the Apache License version 2. It is coded in C++, Ruby and Shell. The network is managed and directed by the administrator. Storage, the default copy of the virtual machines is accessed via SSH. OpenNebula maintains authentication through LDAP [14]. OpenNebula is a simple yet powerful turnkey solution that was designed to help companies to build simple, cost-effective, reliable, open enterprise clouds on existing IT infrastructure. It is the cloud management tool that orchestrates storage, network and virtualization technologies to deploy dynamic placement of services. The powerful of OpenNebula resides in its design which is flexible and modular. It allows integration with different storage and network infrastructure (private, public and hybrid) and supports various hypervisor technologies like KVM, Xen and VMware [2]. OpenNebula cloud infrastructure provides users with an elastic platform for fast delivery and scalability of services and also support Public cloud by providing cloud interfaces and functions to expose its functionality for virtual machine, storage and network management [13].

- OpenStack is an open-source cloud computing software developed and maintained by an open community of developers and engineers under the auspices of the OpenStack foundation[15]. OpenStack began in 2010 as a joint project of Rackspace Hosting and NASA and it has enormously grown and is integrated by 850 companies and 4500 individual members. It is currently supported by major tech industry players, ranging from HP, Dell , IBM, RackSpace , NASA , Cisco, NEC, AT&T ,Bull , EMC, Brocade and dozens of other companies[16]. OpenStack is a collection of open source software projects that cloud computing technologist can use to setup and run their cloud compute and storage infrastructure[13].It produces different solutions for numerous types of cloud which are simple to implement highly scalable and rich in functionality[17]. OpenStack has great potential due to its architecture and community and the support of its partners. All codes are licensed under Apache 2 license. OpenStack has many characteristics; it is scalable, compatible and flexible because it supports most virtualization solutions of the market and it uses different drivers to interface with a maximum number of hypervisors (Xen, KVM, HyperV, Qemu). This project is dedicated to providing the computer industry with the opportunity to build a hosting architecture and massive scalability and is completely an open source, while it overcomes the constraints of the use of proprietary technologies [14].

Open Source Softwares are software with their source code

available to the user with or without fee. The Open source cloud platform provides an alternative to end-user for improved scalability, portability, flexibility and On-demand services [18]. We have compared the three most popular and commonly used open source software (Eucalyptus, OpenStack and OpenNebula).The summarization and comparison allow users to choose better services according to their requirement and to make more unified decision on the open source cloud platform according to their compatibility, scalability, interfaces, requirement and etc. According to this comparative study, it appears that the best solution is OpenStack; it can become the reference solution of open source cloud computing because the architecture analysis and its characteristics feature show that it is useful to deploy large-scale cloud deployments for private, public and hybrid cloud and that too economically. Openstack being used and supported by various commercial and non-commercial houses is a proof for the standardization and maturity of Openstack.

OPENSTACK

A. Openstack Architecture

OpenStack mainly consists of three core software projects which are OpenStack Compute Infrastructure (Nova), OpenStack Object Storage Infrastructure (Swift) and OpenStack Image Service Infrastructure (Glance)[18]. Along with these three, dashboard becomes an important component in providing interface to administrators and users for provisioning and release of resources. These components and their interaction with user's application and underlying hardware over which other openstack services do run can be represented as shown in figure 3[19].

Openstack compute is developed to provide on-demand access to compute resources by provisioning and managing large networks of virtual machines to provide scalable cloud computing platform[14]. Openstack storage provides objects storage to be used for storing necessary images to run virtual machines or virtual instances [19]. Openstack network provides necessary services which are used for communication within virtual machine i.e. inter-VM and external to virtual machines[17].

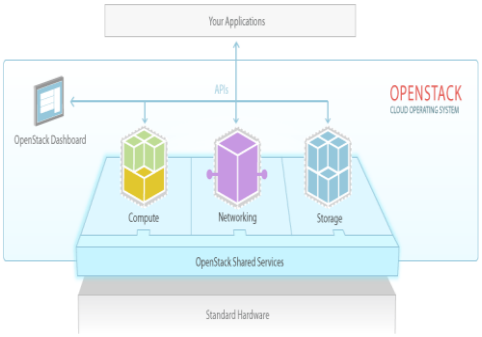

Figure 3: Openstack Architecture

B Openstack Components

OpenStack is an ecosystem aimed at providing flexible cloud computing applications; hence, it consists of series of interrelated projects delivering various components for a cloud infrastructure solution: OpenStack Compute (Nova), OpenStack Image Service (Glance), OpenStack Object Storage (Swift), Network Service (Quantum), OpenStack Block Storage (Cinder), OpenStack Identity (Keystone) and OpenStack Dashboard (Horizon).Relations between these components are shown in Figure 4.

- **Compute (Nova)** is the primary computing engine behind OpenStack. It is used for the large-scale provisioning services and management of virtual machines and other instances to handle computing tasks. It allows the user to create, manage and deploy VMs using a programmable API[2].
- **Object Storage (swift)** is a storage system that provides a scalable and highly available object storage service that distributes, stores the data of users and manages stored user data[20].
- **Identity (Keystone)** provides identity services for OpenStack. It is essentially a central list of all of the users of the OpenStack cloud. It is responsible for handling authentication and authorization of all the services throughout the entire cloud by providing identity, token, catalogue and policy services[2].
- **Block Storage (cinder)** is a block storage component for compute instances that Provides software-defined block storage consumable by Nova Virtual Machines[15].
- **Networking (Neutron)** provides the networking capability for OpenStack. It offers various networking services to cloud users such as IP address management, DNS, DHCP, load balancing, and security groups (network access rules, like firewall policies) [2]. This Component helps to ensure that each of the components of an OpenStack deployment can communicate with each other.
- **Image (Glance)** provides catalog and repository service for virtual disk images. Glance allows these images to be used as templates when deploying new virtual machine instances[15].
- **Dashboard (Horizon)** provides an intuitive web interface for users and administrators who can have a look at what is going on in the cloud, and to manage it as needed[2].

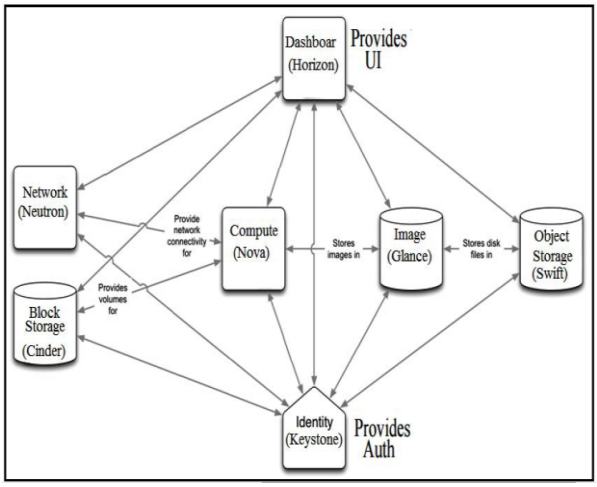

Figure 4: OpenStack main components' relations

PROPOSED APPROACH

The proposed approach consists of designing and implementing a framework which provides data security to the users/clients using fully homomorphic encryption technique. This framework is based on security as a service concept. It is composed of two clouds: A private cloud as a trustable third party that allows encryption/decryption of the data and a second public cloud dedicated for storage where the users can store and manage their data (Figure 5). We propose to implement the first cloud using Openstack platform that controls large pools of compute, storage, and networking resources throughout a data center.

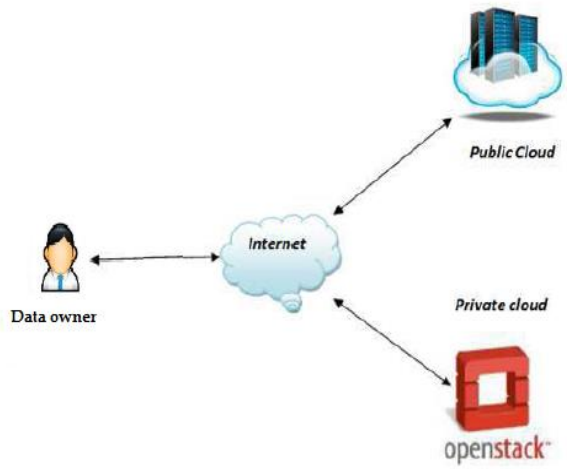

Figure 5: Proposed architecture

The basic idea of this approach is encrypting the data with a fully homomorphic encryption scheme that was implemented on private cloud before moving it on the public cloud. Our approach provides to the customer the possibility to perform arithmetic operations on his data without decryption and compromising the confidentiality of the data. Before sending the data to the cloud provider, the customer sends them to the openstack cloud to crypt them using FHE. After that, he stores the encrypted data in the remote server of the cloud provider. When the customer want to execute some computations on these encrypted data (such as search), he can send a request to the cloud provider asking the calculations of f(a,b) for example. The cloud provider performs the required computations asked by the user without decrypting the data (it has only the ciphers of a and b) and sends him back the result which is encrypted too. To decrypt the result of the computations, the customer sends it to the openstack cloud for decryption and got the same result as it has carried out the computations on the raw data. Figure 6 illustrates the flow of work of using FHE to secure cloud computing.

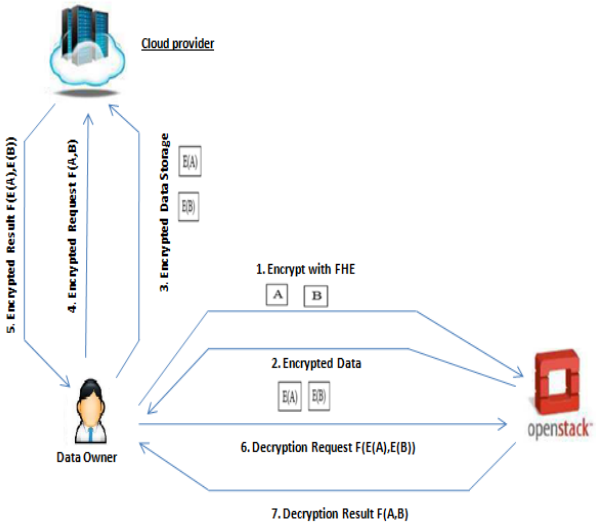

Figure 6: Applying FHE to secure cloud data (flow of work)

The fully homomorphic encryption proposed requires more processing time and memory than the same operations on unencrypted data; it runs slow due to the need of a faster fully homomorphic encryption schemes[21]. To speed up the performance of FHE, we propose an implementation of a parallel processing of Gentry's encryption on the cloud provider. This approach dispatches and splits the operations on FHE encrypted data between a numbers of processing engines. Ryan et Al [22] demonstrates that the parallel processing of Gentry's encryption improves the performance better than the computations on a single node. The figure 7 shows the client-server model of parallel processing of the Gentry's encryption.

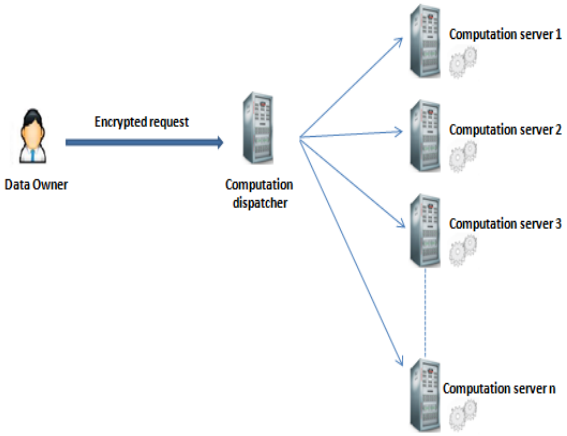

Figure 7: Dispatcher Process inside the Cloud Provider

CONCLUSION

The security concern is the major drawback of widespread adoption of cloud computing technology by organizations that use sensitive and important information. Security of cloud computing based on fully homomorphic encryption is a new concept of security which enables performing computations on encrypted data without the need to the secret key. The Fully Homomorphic Encryption represents a big step in modern cryptography and is the best solution to secure the client data in cloud computing. In this paper, we have proposed a new framework based on security as a service concept including the private cloud OpenStack platform. Our security mechanism is based on fully homomorphic encryption algorithm which we have optimized by implementing a parallel processing of Gentry's encryption to reduce processing time and memory consumption.

Open Source Softwares are software with their source code available to the user with or without fee. The Open source cloud platform is most important which that provides an alternative to end-user for improved portability, flexibility and scalability. These platforms are used for many reasons, each of which requires a different architecture and characteristics. This paper presents also a comparative study on several open-source cloud computing software which are OpenNebula Eucalyptus and OpenStack that are consider the three most popular and commonly used open source software. The results of such analyses could help users to make more unified decisions on the open source cloud platform according to their compatibility, scalability, interfaces, requirement and etc. Typically, open source projects are innovative, with aggressive release cycles that push the technology forward. According to comparative study, Openstack shows it is useful to deploy large-scale cloud deployments for private, public and hybrid cloud and that too economically. Therefore, our proposed architecture for providing security based on OpenStack platform.

On the basis of the promising findings presented in this paper, work on the cloud security optimization is continuing and will be presented in future papers.

REFRENCES

[1] S. Ristov, M. Gusev, and A. Donevski, .2014, "Security Vulnerability Assessment of OpenStack Cloud," 2014 Sixth International Conference on Computational Intelligence, Communication Systems and Networks, pp. 95–100.

[2] S. Ismaeel, A. Miri, D. Chourishi, and S. M. R. Dibaj,.2015, "Open Source Cloud Management Platforms: A Review," 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, pp. 470–475.

[3] Á. Rocha, A. M. Correia, H. Adeli, L. P. Reis, and S. Costanzo, Eds., 2017, "*A View of OpenStack: Toward an Open-Source Solution for Cloud*," vol. 569. Cham: Springer International Publishing.

[4] P. V. Parmar, S. B. Padhar, S. N. Patel, N. I. Bhatt, and R. H. Jhaveri,.2014, "Survey of various homomorphic encryption algorithms and schemes," *Int. J. Comput. Appl.*, vol. 91, no. 8.

[5] I. Jabbar,.2016, "Using Fully Homomorphic Encryption to Secure Cloud Computing," *Internet Things Cloud Comput.*, vol. 4, no. 2, p. 13.

[6] Pascal Paillier,.1999, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," J. Stern (Ed.): EUROCRYPT'99, LNCS 1592, pp. 223-238.

[7] D. Boneh, E.-J. Goh, and K. Nissim,.2005, "Evaluating 2-DNF formulas on ciphertexts," in *Theory of Cryptography Conference*, pp. 325–341.

[8] C. Gentry and others,.2009, "Fully homomorphic encryption using ideal lattices.," in *STOC*, vol. 9, pp. 169–178.

[9] Z. Brakerski and V. Vaikuntanathan,.2011, "Efficient Fully Homomorphic Encryption from (Standard) LWE," 2011 52nd Annual IEEE Symposium on Foundations of Computer Science, pp. 97–106.

[10] S. Bajpai and P. Srivastava,.2014, "A fully homomorphic encryption Implementation on cloud computing," *Int. J. Inf. Comput. Technol. ISSN*, pp. 974–2239.

[11] S. Goldwasser and S. Micali,.1984, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299.

[12] N. Jayapandian, A. M. Z. Rahman, S. Radhikadevi,

and M. Koushikaa,.2016, "Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption," in *Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), World Conference on*, pp. 1–4.

[13] R. Kumar, N. Gupta, S. Charu, K. Jain, and S. K. Jangir,.2014, "Open source solution for cloud computing platform using OpenStack," *Int. J. Comput. Sci. Mob. Comput.*, vol. 3, no. 5, pp. 89–98.

[14] O. Sefraoui, M. Aissaoui, and M. Eleuldj,.2012, "OpenStack: toward an open-source solution for cloud computing," *Int. J. Comput. Appl.*, vol. 55, no. 3.

[15] K. A. Torkura, F. Cheng, and C. Meinel,.2015, "Application of quantitative security metrics in cloud computing," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 256–262.

[16] X. Wen, G. Gu, Q. Li, Y. Gao, and X. Zhang,.2012, "Comparison of open-source cloud management platforms: OpenStack and OpenNebula," *Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on*, pp. 2457–2461.

[17] M. A. Ismail, M. F. Ismail, and H. Ahmed,.2015, "Openstack Cloud Performance Optimization using Linux Services," *Cloud Computing (ICCC), 2015 International Conference on*, pp. 1–4.

[18] S. Yadav,.2013, "Comparative study on open source software for cloud computing platform: Eucalyptus, OpenStack and OpenNebula," *Int. J. Eng. Sci.*, vol. 3, no. 10, pp. 51–54.

[19] R. Kamboj and A. Arya,.2014, "OpenStack: open source cloud computing IaaS platform," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 5.

[20] J.-M. Kim, H.-Y. Jeong, I. Cho, S. M. Kang, and J. H. Park,.2014, "A secure smart-work service model based OpenStack for Cloud computing," *Clust. Comput.*, vol. 17, no. 3, pp. 691–702.

[21] O. Zibouh, A. Dalli, and H. Drissi,.2016, "Cloud Computing Security Through Parallelizing Fully Homomorphic Encryption Applied to multi-cloud Approach," *J. Theor. Appl. Inf. Technol.*, vol. 87, no. 2, p. 300.

[22] R. Hayward and C.-C. Chiang,.2015, "Parallelizing fully homomorphic encryption for a cloud environment," *J. Appl. Res. Technol.*, vol. 13, no. 2, pp. 245–252.