Journal of Theoretical and Applied Information Technology
20th May 2016. Vol.87. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CLOUD COMPUTING SECURITY THROUGH PARALLELIZING FULLY HOMOMORPHIC ENCRYPTION APPLIED TO MULTI-CLOUD APPROACH

[1]OUADIA ZIBOUH, [2]ANOUAR DALLI, [3]HILAL DRISSI

[1,3]Laboratory of Systems Analysis, Information Processing and Integrated Management,
High School of Technology EST-Salé, Mohammed V University Rabat, Morocco

[2]Department of Telecommunications and Networks Engineering,
National School of Applied Sciences-Safi, Cadi Ayyad University Marrakesh, Morocco

E-mail: [1]ouadia.zibouh@gmail.com, [2]anouar_dalli@yahoo.fr, [3]hilaldrissi@gmail.com

ABSTRACT

Cloud computing represents a major change in the way IT resources are utilized and creates value for businesses. It is the future of information technology that offers many benefits such as flexibility, efficiency, scalability, integration and cost reduction. However, the security concern is the major drawback of widespread adoption of this technology by organizations that use sensitive and important information. Therefore, the main aim of this paper is to propose a new framework to secure cloud computing, prevent security risks and improves the performance and the time of data processing .This framework combines between various powerful security techniques such secret sharing schema, Fully Homomorphic Encryption (FHE), multi cloud approach and the implementation of a processing dispatcher which distributes a set of operations on FHE encrypted data between a number of processing engines.

Keywords: *Could Computing, Security, Multi-Clouds, DepSky, RACS, HAIL, ICStore, FHE*

1. INTRODUCTION

Cloud computing describes highly scalable computing resources to deliver applications and services in an effective manner. There are various definitions of cloud computing, but the definition provided by The National Institute of Standards and Technology (NIST) seems to cover all its essential characteristics: "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*."[1]. Cloud computing allows the customers to have access to computing resources and storage through the internet from anywhere at any time on any device without needing the knowledge, expertise or control over the infrastructure and without caring about the management and maintenance issues of the resources. Resources of cloud computing can be quickly and dynamically provided on demand and effortlessly scaled up with all the necessary processes, services and applications like model of allocation and consumption. NIST describes five essential characteristics, three cloud service models, and four cloud deployment models for the cloud computing as shown in Figure 1. The use of cloud computing is rapidly increased in many organizations and starts to be a dominant paradigm for business systems. According to Verizon's report, which is based on survey data from the company's cloud customers and outside researchers, the enterprise cloud adoption is growing spread and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

87% of the enterprises surveyed run at least one mission-critical application in the cloud, up from the 71% in 2014 and 69% of these enterprises confirmed that they used cloud computing to re-engineer one or more of their business processes and find new opportunities to grow [2]. This increase in cloud computing environment also increases security challenges for cloud providers. Ensuring the security of sensitive and important information in cloud computing is the major and high priority of cloud providers in order to increase their reliability and to reach the level of maturity expected by their customers. Recently, due to the potential problems and the limitations of single cloud such as service availability failure, vendor lock-in and the risk of malicious insider attack, some researches proposed the multi-cloud approach which builds a single virtual cloud storage system by using a combination of several commercial cloud storage services. Other researches proposed to crypt data before sending it to the cloud using a cryptosystems based on Homomorphic Encryption in order to resolve the problem of the need of distant calculations to perform on cloud provider but this proposition has a very high impact on performance and memory utilization.

The remainder of this paper is organized as follows: Section 2 discusses security issues related to the data security and privacy aspects in cloud computing, such as data integrity, data confidentiality and service availability. Section 3 analyses a virtual storage cloud system called DepSky which is a multi-clouds mechanism that ensures better availability, integrity and confidentiality of data. In addition, it presents comparative study of security mechanisms in multi-clouds. Section 4 describes the proposed approach to decrease cloud security risks and improve the performance of processing done on sensitive data users. Section 5 concludes the paper.

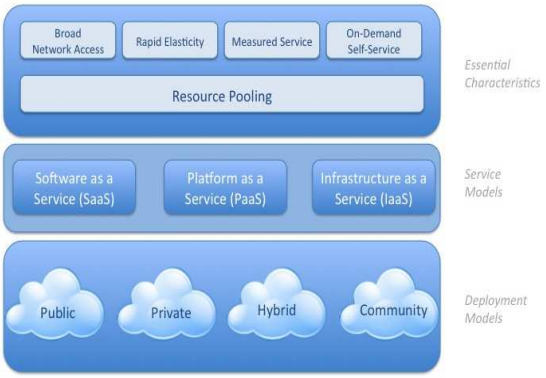

Figure 1: Visual Model of Cloud Computing (NIST Definition)

2. CLOUD SECURITY ISSUES

Security issues of data stored in cloud are still the major obstacle to a larger adoption of Cloud computing. Cloud computing comes with numerous security issues because it consists of various technologies including databases, network, operating systems, virtualization, resource scheduling, transaction management, load balancing concurrency control and memory management. Because of the wide use of these technologies, a small security weakness in one of these technologies can bring down the whole system. Cloud provider offers various cloud services as IaaS, PaaS, SaaS and the models like public, private, hybrid, Community (For more details, refer to NIST document [1]). Each service and model has cloud security issues. Hence the security issues can vary according to the cloud delivery models and the service used by cloud user organizations. The security responsibilities in the cloud are shared between the provider who should secure the service provided by them and also manages the customer's identity management and the consumer who is using the service.

2.1 Data Security

2.1.1 Data confidentiality and privacy

In a cloud computing environment, confidentiality is a key concern when the data stored in the cloud are sensitive such as bank details, documents healthcare, financial service. A customer of any service cloud should be aware of the risks associated with data security e.g., data loss and data theft [3].The risk can be caused by a malicious insider (administrator who work with Cloud Provider) or by a malicious outsider (hackers and attackers who exploit the API and weakness) or by a partner. The attacks that come from outsider are less harmful than the insider attacks because in the latter sometimes it is difficult to identify the attack [4]. According to Verizon's annual Data Breach Investigations Report based on actual data breaches, the overall proportion attributed to attacks coming from external, internal, and partner actors stays almost the same over the last five years as shown in the figure 2 in which more than 80% of breaches are attributed to external threats. Approximately 18% are from internal actors, and tiny percent are attributed to partners [5].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

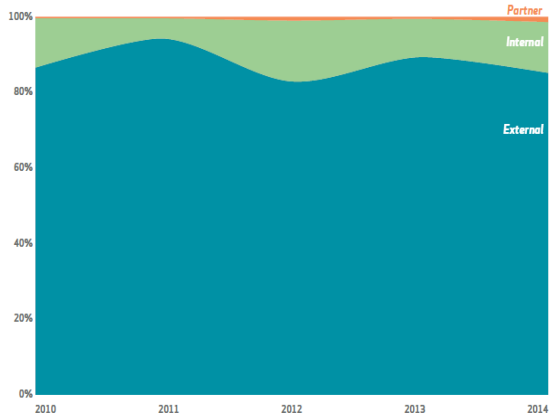

Figure 2: Actor Categories Over Time By Percent Of Actors [5]

Several reports related to privacy of data have been outward in recent years despite the security mechanisms deployed by the service providers [6]. One of the powerful security measures used by the CSP (Cloud Service Provider) to ensure customers' data safety is the encryption of the data stored in the cloud and the security of the keys is the potential weakness of this mechanism. For example, some cloud providers keep a copy of the encryption key and hide this information from their customers, they can potentially decrypt and access all the data stored in their servers such as Apple that has a service called "iMessage" that handles text messages in the cloud. They ensure that all messages are encrypted end to end but they don't tell their customers that they are legally required to keep a copy of the key [3]. The process of encrypting data by CSPs requires the clients to fully trust the CSPs because the keys are managed by them. To ensure the safety of sensitive and confidential data in the cloud, some researches recommend to the clients to encrypt the data before storing it to the cloud. But this approach requires an effective and secure key management approach in the responsibility of the clients because they can lose the data forever in the case of the loss of key[7]. To secure storage and treatment of data, we need a powerful cryptographic technique that respects some criteria, for example, it should guaranty a reasonable time of the treatment of any request asked by the client and a minimum size of an encrypted data which will be stored on the Cloud server and that offers the possibility to perform distant calculations on encrypted data without decrypting it and thus expose it to attack because the clients can need from time to time to perform processing on their data. Maha et Al [8] propose to crypt data before sending it to the cloud using a cryptosystems based on Homomorphic Encryption which allows performing computations on encrypted data without decrypting, this technique avoid the problem to provide the encryption key to the cloud provider in order to perform the calculations required. 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. Ryan et Al [9] propose an implementation of a parallel processing of Gentry's encryption that dispatches and splits the operations on FHE encrypted data between a number of processing engines and they demonstrate that this implementation improve the performance better than the computations on a single node.

Another security risk is that some government authorities such as National Security Agency (NSA) can force cloud service providers to install backdoors in their systems to allow them to access to data customers by providing them an encryption key. The example of prism scandal has a very high impact on future of cloud security specially maintenance of privacy, government policy, and data theft [3]. Many cloud environments do not encrypt their data to improve efficiency; they store it in plain text in the disk. This is a severe threat for critical data, a rogue employee of the provider or unauthorized operating system users can access sensitive information by inspecting the contents of system files presented in the disk [10].

Confidentiality of data can be breached in transit or while it is stored at the cloud storage. When customers send data to the cloud, it may be attacked by Man-in-the-Middle who creates an independent connection and communicates with the cloud user on its private network where the attacker can interrupt, intercept, modify data user [4]. In [11] Confidentiality can be also affected by hacking users' account such the Amazon cloud service. The stolen Amazon account password allows the hacker to breach the totality of account's instances and resources. The possibility to reset the Amazon account by email is another security risk that threatens the privacy of data in the case of the user's email has been hacked.

Another security risk in the cloud computing is multi-tenancy that implies sharing of resources, storage, memory, services and applications with other tenants. It means that customers' data may be stored in the same physical machine which can be exploited by the adversaries to launch various attacks such as data/computation breach, flooding attack, etc [3].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.1.2 Data availability

High availability of services, data and applications is among the most important driving forces behind switching to the cloud service. It is the key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models. Hence Companies should highlight the availability of services in the service level agreement to ensure access to their data [12]. Amazon mentions in its licensing agreement that it is possible that the service might be unavailable at any time and there will be no charge to the Amazon Company for this failure [13][14]. Garima et Al [4] give examples of attacks that can affect the data availability such Malware Injection Attack in which the hacker introduce a malicious code into the data transferred between cloud provider and customer. As a possible consequence of this attack, the cloud service may be unavailable until the completion of the job that was maliciously introduced. Another attack which could have a negative impact on availability is Distributed Denial of Service (DDoS) attack in which a legitimate customers and partners are deprived of the services and resources they would normally expect to have access to by absorbing all available bandwidth. This attack have a large impact on business operations such as the loss of revenue opportunities, decreased productivity or damage to company's reputation [7].

2.2 Security Assurance in Service Level Agreements

Storing critical and sensitive data with cloud providers comes with serious security risks which prevents companies to adopt cloud despite its advantages. Usually, in order to guarantee a certain level of quality of service (QoS) which is essential to users' business operations Service Level Agreements (SLA) which specify contracts between providers and users and involves all the terms and conditions are commonly used. Unfortunately, Most of major commercial cloud vendors such Amazon S3 (Amazon Simple Storage Service) provides a quality of service limited to performance, availability, durability and persistence of data without security and reliability assurance in their SLAs [15]. They are mainly focused on very few terms that related to security, mainly disaster recovery and business continuity [16].

SLA contracts can be either non-negotiable agreements which is a standard form contracts or customized negotiable contracts tailored to fit the specific requirements of the cloud service customer. Public cloud providers often offer a non-negotiable SLA which does not meet business requirements and may not be acceptable for organizations that have critical data [17]. SLA plays a very important role in cloud computing, to maintain the quality of service; SLA has to be developed to include the security and privacy assurances in order to meet customer requirements.

3. MULTI-CLOUD APPROACH

Depending on a single cloud provider is becoming less popular with customers due to potential problems such as service availability failure, the possibility of malicious insiders attacks and the customer's risk for the so-called "vendor lock-in" problem. In order to mitigate this risk and provide resistance to loss or corruption of sensitive data at cloud providers and provide also several potential benefits, such as high availability, reliability, fault tolerance, business continuity and disaster recovery, various concepts applying the so-called "cloud of clouds" or in other words, "interclouds" or "multi-clouds" approach – have been proposed.

Multi clouds approach is a cloud storage architecture that builds a virtual cloud storage system by using a combination of diverse commercial cloud storage services. Thereby, the data to be stored is split into various blocks and distributed among different cloud storage providers in a redundant way. There are two ways for redundancy. The first one is naively replicating the data to several providers by storing an entire copy of a file at each provider and the second way is dispersing suitably encoded data in such a way only a certain threshold of file fragments is required for reconstruction of a file [13].

3.1 Depsky System

An example of Multi-cloud architecture is DepSky architecture. It is a combination of several different storage clouds. This system improves the availability, confidentiality and integrity of stored data in the cloud by encrypting, encoding and replicating all the data on a set of different clouds. This architecture addresses the highs important limitations in the single cloud, it addresses availability issue by replicating all the data in a set of clouds and as a result the data can be retrieved correctly even if some of the clouds corrupt or lost data. It addresses the loss and corruption of data issue by using Byzantine fault-tolerance replication to store data in multi-clouds. It addresses the loss of confidentiality issue by employing a secret sharing schema and erasure codes to ensure that all data that will be stored in a multi-clouds are encrypted

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and it avoids also the "vendor lock_in" problem by using a set of cloud provider instead of a single one [18]. The DepSky architecture consists of four clouds and each cloud uses its own specific interface. The DepSky algorithm is implemented in the clients' machines as a program library to communicate with each cloud as shown in the figure 3. The DepSky library offers an object store interface that allows reading and writing operations with the storage clouds and their multiple side clients and as a result, the data format is accredited by each cloud [19].

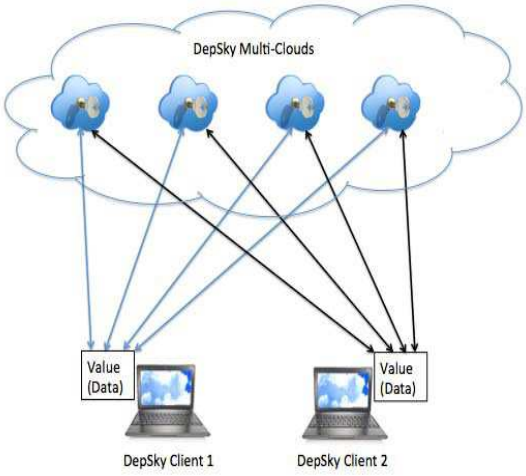

Figure 3: Architecture Of DepSky

The DepSky system provides two versions, namely DepSKY-A and DepSKY-CA. DepSky-A (Available DepSky) replicates the data into different cloud providers by using quorum techniques in order to improve the availability and the integrity of the stored data in the cloud. However, the confidentiality is the major drawback of this algorithm because it doesn't encrypt the data stored in the cloud. DepSky-CA (Confidential & Available DepSky) addresses this limitation by encrypting data before storing them in the multi-Clouds using secret sharing scheme and erasure code techniques. After the encryption and the encoding of the data, it is divided into blocks as f+1 blocks are necessary to recover the original data and f or less blocks were not enough to retrieve the original stored data. Lastly, a different coded block is stored in each cloud together with a different key share that was computed from the encryption key using threshold secret sharing (Figure 4) [11].

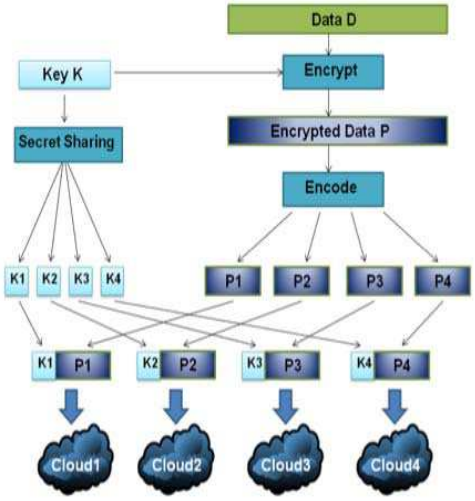

Figure 4: DepSky-CA Algorithm

3.2 Comparative Study of Security Mechanisms in Multi-clouds

Recently some researches in the use of multi-cloud providers to maintain security and mitigates the limitations of individual clouds have built protocols for interclouds. RACS (Redundant Array of Cloud Storage) for example, utilizes RAID sample techniques that are normally used by disks and file systems, but for multiple cloud storage. It is a cloud storage proxy that transparently distributes a user data across multiple cloud storage providers. This reproduction allows clients to tolerate outages and economic failures. It avoids vendor lock-in problem and its associated risks. Differently, from DepSky, the RACS system does not try to solve security problems of cloud storage and it does not provide any mechanism of detecting and recovering data corruption or ensuring data confidentiality. Moreover, it does not provide updates of the stored data [11]. HAIL (High Availability and Integrity Layer) is another example of a protocol that controls multiple clouds. HAIL is a distributed cryptographic system that permits a set of servers to ensure that the client's stored data is recoverable and integral. HAIL provides a software layer to address availability and integrity of the stored data in an intercloud. Differently, from DepSky, HAIL requires executing code in cloud servers and it does not support the management of different versions of data [20]. Cachin et al.[21] present a design for intercloud storage (ICStore), which is an approach closer than RACS and HAIL as a dependable service in multiple clouds. This mechanism contains various theories and protocols that were developed in order to target different dependability

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

aspects (confidentiality, integrity, reliability and consistency) of the data stored in clouds. Differently from DEPSKY, ICStore does not ensure the confidentiality of data stored in the cloud because it isn't based on the secret sharing algorithm. However, it is not clear if information-efficient secret sharing or some variant of this technique could substitute the erasure codes employed on these protocols.

The overall comparative analysis of the different security mechanisms used in the multi-clouds demonstrates that the depsky architecture is the most reliable mechanisms due to its ability to reduce breaches and other security issues and to ensure a better security (Confidentiality, Integrity and Availability) of data stored in different cloud providers (as shown in table 1). It presents an experimental evaluation with several clouds that is different from other research on multi clouds.

Table 1: Comparative Study of Security Mechanisms in Multi-clouds

	Data Integrity	Service Availability	Data Confidentiality
Depsky	√	√	√
RACS			
HAIL	√	√	
IC Store	√		

4. PROPOSED APPROACH

Most of the cloud providers propose to their customers to encrypt their data before sending them to the cloud. However, the cloud provider requires the decryption key when the clients need to perform computations on their data. Consequently, the data becomes vulnerable during computation and the cloud provider can preserve all the decrypted data. So, there is a real need to use an effective encryption algorithm that performs computations on encrypted data without decryption in order to enforce the data security. Homomorphic encryption is the crypto system that can resolve this problem due to its capability to perform computations on encrypted data without decrypting it whereby the encrypted results can only be decrypted by the client who requests the computations and its decryption produces the same result as performing the same computations on the original data. Fully homomorphic encryption is a very important notion for cloud computing security. It allows companies and organizations to store their data in the cloud and benefit of the cloud provider's analytic services without providing the key encryption to cloud providers. In recent years, a number of approaches to fully or partially homomorphic encryption have been proposed. According to the comparison of the Homomorphic Encryption cryptosystems (RSA, Paillier, El Gamal, Goldwasser-Micali, Boneh-Goh-Nissim and Gentry) on a Cloud Computing platform [8], The Gentry's fully homomorphic seems to be the most appropriate algorithm for the cloud because it is able to execute all types of mathematical operations on encrypted data. However, the fully homomorphic encryption requires more processing time and memory than the same operations on unencrypted data, it runs slow due the need of a faster fully homomorphic encryption schemes. To speed up the performance of FHE, Ryan et Al [9] proposed an implementation of a parallel processing of Gentry's encryption that dispatches and splits the operations on FHE encrypted data between a number of processing engines. This implementation was tested in a private cloud computing environment that consists of two computation servers providing the virtualized infrastructure for execution and the time taken to perform the calculations was measured with four levels of parallelization (1, 2, 4, and 8 processing engines). Each computation server provides 4 processing engines and the trials with 1, 2, and 4 nodes occurred only on the primary computation server. The two computation servers were connected by a wireless network. In order to evaluate cloud computing of the Gentry's encryption algorithm a client-server model as shown in the figure 5 was created and to support parallel processing of the Gentry's encryption a distributed algorithm was developed and tested by performing three computations on cloud system in such a way all the computations are using the same set of data which contain 20 random 8-bit integers.

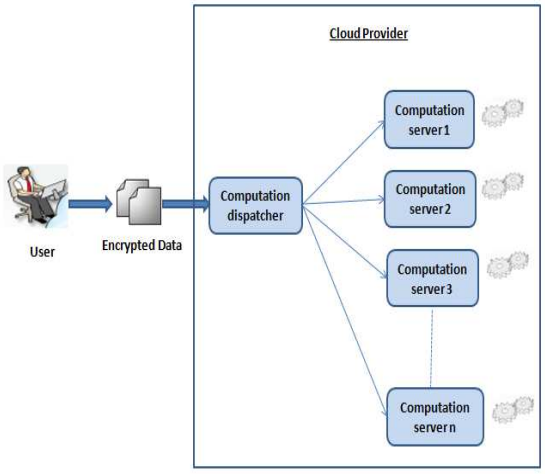

Figure 5: Dispatcher Process Inside The Cloud Provider

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The first experiment consists on computing the sum of these 20 integers by splitting them into 10 pairs and calculating the sum of each pair and the resulting 10 integers were then split into 5 pairs, and summed, and so on. The second experiment is to compute the vector product of the integers by first taking the pair-wise product of the integers that producing 10 integers. These integers were then summed. The third experiment is to compute the variance of the integers by taking the square of the sum of the integers plus the sum of the squares of the integers [9].

The time to perform the three evaluations (Sum, Vector product and Variance) on 1, 2, 4, and 8 compute nodes is shown together in Table 2.

Table 2: Comparative Nodes Vs. Time In Microseconds[9].

Node size	Processing time (µs)		
	Sum	Vector product	Variance
1	34.90	952.17	2496.62
2	25.28	541.92	1599.50
4	24.85	491.50	1459.75
8	32.08	337.80	1052.45

The sum experiment showed good speedups while all computation servers were on the same computer as the dispatcher, but decreased when computation servers distributed over 8 nodes and two computers. This decrease is most likely due to network transfer time coupled with the small amount of time taken to perform the sum operations.

The vector product and variance experiments showed good speedups in the more complex and time consuming whenever we add more nodes despite the computations done on the same or separate computer. The speedup of the vector product and variance experiments when distributed over 8 nodes were respectively 2.8187 and 2.3722.

Despite the decrease performance of the sum trial when computation servers distributed over 8 nodes on a separate computer, the speedup of the vector product and variance circuits suggests that the proposed algorithm is useful to improve the performance and to decrease the time to evaluate the homomorphic circuits as we increase the processing engines in the system [9].

Due to the limitations of single cloud and the benefits offered by multi-clouds architecture and due to the need of performing distant calculations on encrypted data with high security and performance, we propose to integrate parallel processing of the Gentry's fully homomorphic encryption algorithm in DepSky system in such a way FHE integrates in the secret sharing scheme and the parallel processing of this new algorithm in each cloud provider of depsky. The proposed approach will decrease cloud security risks and improve the performance of processing done on sensitive data users.

5. CONCLUSION

The purpose of this work is to survey the cloud security which is the main obstacle of cloud adoption by organizations that hesitate to move their workload to cloud computing. Furthermore the limitations of single cloud, advantages of multi cloud and analyze of different security mechanisms in multi clouds approach were addressed in this paper. Then, we have proposed a new architecture to secure data storage and to improve the performance of encrypted data processing engines by integrating parallel processing of the Gentry's fully homomorphic encryption algorithm in DepSky system which is the most reliable multi clouds mechanism that decreases the security risk on cloud computing by ensuring better confidentiality, integrity and high availability of sensitive data users stored in the cloud. This proposed approach enables the user to take advantage of depsky multi cloud mechanism and the speed of performance of parallel processing of Gentry's encryption.

REFRENCES:

[1] A. Kumar, "NIST- The Definition of Cloud Computing-2013", *Asian Journal of Multidisciplinary Studies*, vol. 2, no. 1, 2014.

[2] Verizon, "State of the Market: Enterprise Cloud 2016", November, 2015, pp. 3, 8.

[3] P. Mosca, Y. Zhang, Z. Xiao, and Y. Wang, "Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services", *International Journal of Communications, Network and System Sci*ences, vol. 07, no. 12, 2014, pp. 529–535.

[4] G. Gupta, L. P.R, and S. Sharma, "A Survey on Cloud Security Issues and Techniques", *International Journal on Computational Sciences & Applications,* vol. 4, no. 1, February 2014, pp. 125–132.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[5] Verizon, "2015 Data Breach Investigations Report", May 2015, p. 4.

[6] F. S. Al-Anzi, A. A. Salman, and N. K. Jacob, "New Proposed Robust, Scalable and Secure Network Cloud Computing Storage Architecture", *Journal of Software Engineering Applications,* vol. 07, no. 05, 2014, pp. 347–353.

[7] F. Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions", *Procedia Computer Sci*ence, vol. 37, 2014, pp. 357–362.

[8] M. Tebaa and S. E. Hajji, "Secure Cloud Computing through Homomorphic Encryption", *International Journal of Advancements in Computing Technology (IJACT*), vol. 5, no. 16, December 2013.

[9] R. Hayward and C.-C. Chiang, "Parallelizing Fully Homomorphic Encryption for a Cloud Environment", *Journal of Applied Research and technology*, 2015, pp. 245–252.

[10] V. N. Inukollu, S. Arsi, and S. R. Ravuri, "High Level View of Cloud Security : Issues and Solutions", *Computer science & Information Technology (CS & IT),* 2014, pp. 51–61.

[11] M. A. AlZain, B. Soh, and E. Pardede, "A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds", *Journal of Software*, vol. 8, no. 5, May 2013.

[12] S. Anbazhagan and K. Somasundaram, "Cloud Computing Security through Symmetric Cipher Model", *International Journal of Computer Science & Information Technology* (IJCSIT), vol. 6, no. 3, June 2014, pp. 57–66.

[13] D. Slamanig and C. Hanser, "On Cloud Storage and the Cloud of Clouds Approach", *IEEE*, *in Internet Technology and Secured Transactions, 2012 International Conference for*, 2012, pp. 649–655.

[14] M. Tebaa and S. E. Hajji, "From Single to Multi-clouds Computing Privacy and Fault Tolerance", *IERI Procedia*, vol. 10, 2014, pp. 112–118.

[15] N. A. AL-SAIYD and N. SAIL, "Data Integrity in Cloud Computing Security", *Journal of Theoretical and Applied Information Technology*, vol. 58, no. 3, 2013.

[16] S. Khaddaj, J. M. Arul, H.-Y. Chung, H.-Y. Ko, M. Dugki, V. K. K. EunmiChoi, A. Budiyono, A. R. Frando, T. Prakash, M. James, and others, "QoS and SLA in Cloud Computing", *International Journal of Emerging Trends in Computing and Communication technology*, vol. 1, no. 1, February 2014.

[17] A. Mathew, "Security And Privacy Issues Of Cloud Computing; Solutions And Secure Framework", *International Journal Multidisciplinary Research*, vol. 2, no. 4, April 2012.

[18] A. Bessani, M. Correia, B. Quaresma, F. André, and P. Sousa, "DepSky: Dependable and Secure Storage in a Cloud-of-Clouds", *ACM Transactions on Storage,* vol. 9, no. 4, November 2013, pp. 1–33.

[19] M. Shrawankar and A. K. Shrivastava, "Security Threat Solution over Single Cloud To Multi-Cloud Using DepSky Model", *IOSR Journal of Computer engineering (IOSR-JCE),* vol. 14, Issue. 1, September - October 2013, pp. 71–76.

[20] S. S. Mirajkar and S. Biradar, "Using Secrete Sharing Algorithm for Ensuring Security in Multi-Cloud Computing", *International Journal of Advanced Researh in Computer Science & Technology (IJARCST),* vol. 2, Issue. 2, Ver. 3, April - June 2014.

[21] M. Shrawankar and A. K. Shrivastava, "Comparative Study of Security Mechanisms in Multi-clouds Environment", *International Journal Computer Applications (0975-8887),* vol. 77, no. 6, September 2013.