EISSN: 2707-0425

East African Journal of Science, Technology and Innovation, Vol. 2 (4): September 2021

Hardware-based security approach for secure distributed cloud data storage and retrieval

[1,2*]MUGISHA E

[1*]Department of Computing and Information System, University of Lay Adventists of Kigali (UNILAK), Kigali, Rwanda
[2]African Center of Excellence in Internet of Things, College of Science and Technology, University of Rwanda (UR), Kigali, Rwanda

***Corresponding author**: emymugi.cis@unilak.ac.rw

Abstract

The East African Community (EAC) recognizes the fundamental role of science and technology in economic development. This led the Partner States to promote cooperation in the development and application of science and technology within the Community. The adoption of cloud computing in East Africa Community member states may induce a number of paths for Internet-based service provisioning to satisfy various demands in the community. However, data privacy and security has turned into crucial issues that resist cloud adoption for the past decades in the area of computerized systems. The dominating issue regarding security and privacy is pointed out on the data accessibility whereby cloud service providers and consumers simply gain access to secret information (data). The issue resulted in the cloud service consumer's fear and slowed down the adoption speed of cloud computing from diverse areas of applications, i.e., governmental, medical and financial institutions; therefore, in this article we address this issue and propose a robust Hardware-Based Security (HBS) approach, whereby the cloud service provider and consumers are limited to simply access any stored data in the cloud data centers. This approach halves data files into data segments and distributes encrypted file segments to different cloud data centers. Our approach is built on Secure Data Distribution (SDD) and Data Retrieval (DR) Algorithms described in a Secure Efficient Data Distribution Model (SEDD). The analysis shows robust data security and less computation power which can resist unauthorized data accessibility with less latency. Therefore, once the East African Community member states adopt a secure cloud services, the development and application of science and technology within the community will boost the sustainable economic development.

Keywords: *Cloud; Community; services; Data Storage; Data distribution; Data retrieval; Data, Security*

Received: 04/06/21
Accepted: 15/09/21
Published: 25/09/21

Cite as: *Mugisha, (2021)* Hardware-based security (HBS) approach for secure distributed cloud data storage and retrieval. *East African Journal of Science, Technology and Innovation 2(4)*

Introduction

The Establishment of the East African Community (EAC) recognizes the fundamental role of science and technology in economic development and demonstrates, in Chapter 16, Article 103, provisions for the member states to advance cooperation in the application and development of science and technology within the community. Article 80, on industrial development, further reinforces the need for the development of science and technology to accelerate socio-economic development in the community. However, building ICT infrastructure within EAC in regard to cloud adoption is still in its early stage EAC (2019). Therefore, must be among the hot topics to be considered in the construction of cloud infrastructure in EAC member states Times Reporter (2012). Generally, EAC member states has been outsourcing their data to cloud

providers and relying on their security parameters, United Nations (2013). There is a need to readiness in terms of data security and privacy in EAC.

Cloud Computing (CC) adoption is rapidly rising and attracting apparent lot of attention in the scientific and industrial research. Gartner (2011) studied CC within ten most leading authoritative technologies as the first and promising expectations in sequential ages by cloud players. CC enables 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.

CC shows a distribution architecture with the main objective of providing convenient data storage and network service, secure and quick services in a virtualized environment and accessed via Internet medium (Zhao *et al.,* 2009); (Zhang *et al.,* 2010). CC advances scalability, agility, availability, collaboration and ability to adapt variations according to request, access and allows possible cost-effective using optimized and effective tools (Cloud Security Alliance 2011; Marinos and Briscoe, 2009; Centre for the Protection of National Infrastructure, 2010; Khalid, 2010). Moreover, CC merges a number of computing technologies; that is to say: Web 2.0, Service Oriented Architecture (SOA), virtualization and several technologies are based on Internet to provide common Internet-based services (applications) online using web browsers to meet tenants needs, as their applications/services and data are stored on the servers/datacenters (Marinos and Briscoe, 2009). Furthermore, CC act as the ageing of these technologies and is a commercial term to constitute that ageing and the services they offer (Centre for the Protection of National Infrastructure, 2010). However, though a number of interests to adopting CC; there exist a number of apparent obstacles to its adoption. That is, security, standardization, privacy and legal trends are the major obstacles for CC adoption (KPMG, 2010).

In addition, CC constitutes a comparative novel computing model. However, there remains doubt regarding how security can be attained to all models, as well as how application' security is moved to the cloud (Rosado *et al.,* 2012). This doubt has systematically guided information administrators to express that security is their priority on CC trends (Mather *et al.,* 2009). Security priorities refer to dangerous domains for instance; multi-tenancy, external data storage, public internet dependence. In relation to traditional computing technologies, the cloud consists of several particular characteristics, i.e. large scale, resource distribution by cloud providers, heterogeneity and virtualized. Therefore, security controls for other IT environment doesn't differ from that of CC. However, since cloud service models are utilized, CC might demonstrate unique dangers to an organization with operational models, together with technologies used to enable cloud services than traditional IT solutions.

Distributed storage service in cloud computing has advanced apparently in the past decades in the provisioning Software-as-service (SaaS) to communities. It has provisioned instant data storage service models. These cloud service models have widely turned applicable solutions in the development of Web services and networks Chang and Ramachandran (2016); (Gai *et al.,* 2015). Moreover, a number of cloud storage providers have managed to lease reliable storage service provisioning with scalable cloud-based storage instances, i.e. (Microsoft's OneDrive *et al.,* 2015); (Gai *et al.,* 2016); Howley (2015). However, the security and privacy issues remain a critical part for cloud storage adoption (Ali *et al.,* 2015); (Chen *et al.,* 2014); (Costa *et al.,* 2015). Nowadays, cloud data might be accessed at the cloud provider side due to the nature of cloud Service Level Agreement (SLA); hence, balancing computation and security is complex and costly (Wu *et al.,* 2013). Consequently, to secure distributed data in the cloud effectively has become a complex issue as a result of cloud vulnerabilities from different network levels which are not completely treated (Gai *et al.,* 2015); (Qiu *et al.,* 2015).

In this article, we focus on the cloud providers and user's offensive behavior that targets other

collocated user's data from cloud data centers. We propose a Hardware-based Security (HBS) approach that can efficiently perform secure data distribution and retrieval services with trusted security measures attached. This approach aims at implementing a trusted platform module (TPM) from the cloud user side. This platform is built on hardware-based level of trust. Therefore, the software defined security is not a concern of TPM capabilities since at this level must be effective during data transmission along application layer. Moreover, during the data encryption process, an encryption key is stored at the user' side TPM. The encrypted data block is distributed to a separate cloud datacenter. Figure 1 shows the architecture design of HBS. Hence, attacks (compromise) against data stored in a hardware defined TPM capabilities will not be successful Microsoft. (2021).

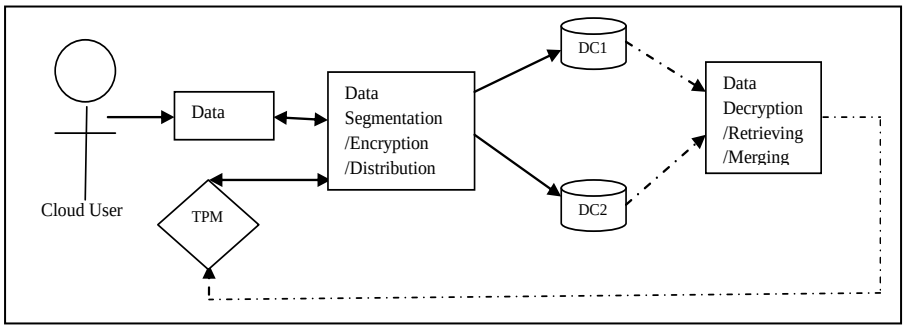

Figure 1. HBS architecture mode

The remainder of this paper is arranged as follows: related work is presented in Section 2, the proposed model is discussed in Section 3; algorithms are given in Section 4; HSB is further discussed in Section 5, and, finally, Section 6 gives the Conclusions of the study.

Related Works

In this section, we look at the previous study on data security in cloud storage systems with regard to our research boundaries, and the theoretical introduction. In addition, it presents current data security issues in cloud storage systems and active techniques of distributed cloud storage. Furthermore, we describe the primary security threats in cloud data storage.

Security in Storage Cloud

Here, the analysis of current surviving security vulnerabilities and threats in CC is described. Expanding, each vulnerability and threat impacts cloud service model or models. Table 1 demonstrates an analysis of vulnerabilities in CC. The analysis contributes a basic interpretation of vulnerabilities, and point out particular cloud service models (SPI) expected to be impacted.

We look at technology-oriented vulnerabilities, where some institutional common vulnerability needs much attention since they harm the security policy of the cloud. Unprofessional strategy of employee recruitment and briefing with regard to security policy (Cloud Security Alliance, 2010); authorized tenants, i.e. cloud executives holds full access to the cloud data. Lacking occasional customer desktop controls which may lead to unauthorized or adversary to open an account with a valid credit card and email. Apocryphal accounts can allow unauthorized or adversary to perform malicious action unknowingly (Cloud Security Alliance, 2010). Lack of security education or guidelines can allow tenants as weak point to pose information security vulnerability (Popovic and Hocenski, 2010).

CC merges a number of new and old technologies such as virtualization, web browsers and web services that leads to the development of cloud concept. In addition to that, given that these technologies are vulnerable to the attacker, it will as well be vulnerable to the cloud, hence compromised. Considering Table 1, it is very

clear that virtualization and data storage are prior critical aspect.

Table 2. Vulnerabilities in cloud computing

Vulnerabilities	Service Model	Description
Data-associated vulnerabilities	SPI	Data may be located or stored in several different jurisdiction with different SLA, from there, data can be accommodated together with hacker's, with no strong separation mechanism, again, tenants are not aware of where their data is located. Given that a tenant decides to leave the cloud, he cannot trust if his data was completely deleted from the cloud. Data storage, access and transmitted are in form of plain text which makes it easy to hackers to access useful information;
Unlimited allocation of resources	SPI	Wrong resource utilization modeling may contribute to over-provisioning.
Vulnerabilities in virtual networks	I	Virtual bridges shared by various VMs.
Unsafe APIs & UI	SPI	Cloud providers extend services via APIs (SOAP or REST & HTTP). The cloud is required to secure its interface so as its service access to be safe. Cloud APIs are still in early evolution as it upgrades timely and that can become a door for an attack.
Vulnerabilities in VMs	I	Virtual Machines have IP addresses visible to all logged in the cloud, this allows hackers to map VM location; Lack of VMs migration control from server to server may result a serious danger.

Moreover, compromising lower layers implies other layers as well. Table 2 summarizes different threats in CC. It also depicts the threats that are inherited from vulnerable technologies merged in cloud environments, and we continue by showing cloud service models that are likely to be compromised by these threats. We look at threats linked to virtualization, resource pool and remote data storage and accessibility.

In cloud storage systems, the data security trend has penetrated into all cloud computing layers, from system management to networks (Yan *et al.,* 2013). Within networks and data storage, various security threats are inherent to cloud storage systems due to several joint technical applications; however, recent studies discovered the security issues and result from different data security views (Liu *et al.,* 2014).

Table 2. Threats in cloud computing

Threat	Service Model	Description

Data leakages	SPI	Data leakages take place during the time tenant's data or information is redirected to a harm address as is in transit, stored, audited or processed.
Data scavenging	SPI	Deleted tenant data can still be restored by hackers, since data cannot be permanently deleted until the device or resource is destroyed.
Service Hijacking	SPI	A service hijack can be done in different ways, i.e. social engineering. If an adversary wins access to a service tenant's important information, he is likely to act malicious actions such as access to secret data, changes data, and reverse services.
Denial of service	SPI	Malicious tenants are anticipated to gain access to all resources. Hence, the cloud will suffer resource availability while other tenants requests.
VM escape	I	This targets hypervisor with the goal of gaining management of the fundamental infrastructure in the cloud.
Customer-data manipulation	S	Tenant's web application abuse by faking data sent from their application part to the cloud server's.
Malicious VM creation	I	A legitimate account might become an adversary by creating a valid VM image with malicious scripts such as a Trojan horse and despite them in the cloud storage.
VM hopping	I	It occurs when a VM is able to gain access to another VM via open vulnerability.
Sniffing virtual network	I	A virtual network packet can be reversed to other VMs by use of ARP spoofing as a result of a harmful VM hopping.
Insecure VM migration	I	Live VMs migration discloses log file contents to the network which allows hackers to access, redirect the VM to unexpected address, hence DoS.
Data leakages	SPI	Data leakages take place during the time tenant's data or information is redirected to a harm address as is in transit, stored and audited.

Pedrycz (2014) have defined data management security as a process of securing data in cloud storage systems using encryption or cryptographic algorithms;

Therefore, an optional or alternative data encryption was considered in (Cao *et al.,* 2014); (Gai *et al.,* 2015) to reduce computing expenses on protecting data in clouds. However, nowadays data management approaches consider that the cloud service providers or cloud users/consumers have no interest in compromising user's data stored on the cloud datacenter. But, assumptions show that there are possibilities that cloud providers or users may retrieve information from user's data, albeit the data are encrypted. Furthermore, protecting and supervising data storage is an added attribute to secure data in the cloud, this accounts data processing event from the clouds. (Li *et al.,* 2013); (Qiu *et al.,* 2016) recommended that the cloud service provider's behavior must be examined, therefore, an Attributed-Based Encryption (ABE) approach was used to secure the privacy of the information while distributing data (in transit) to different clouds. Henceforth, in data storage to achieve privacy protection and data processing is still a challenge. In addition, there are ongoing researches that are seeking to balance the trade-off between them hence minimizing storage systems costs (Liu *et al.,* 2015).

Mass Distributed Storage

Mass Distributed Storage is a technique applied in cloud storage systems (Yu *et al.,* 2015). However, MDS accommodates a number of drawbacks including storage reliability, accessibility, and availability as well as

insecurity. In cloud storage systems, data synchronizations have become challenging as a result of resource allocation restrictions. In this case, the notion of local synchronization into asynchronous SN P systems was presented (Song *et al.,* 2013). In distributed parallel computing resources, they introduced a method to optimize computation power. Moreover, diverse studies Cimino and Marcelloni, (2011) have conducted on business process mending by implementing methods for cloud storage efficiency. For instance, a mobile and agent-based method was introduced to draw or track business production processes. Furthermore, other studies (Yan *et al.,* 2014) emphasized information protection, i.e., access control methods and level of trust management. In (Yan *et al.,* 2014) a secure community instant data access proposal was conducted by employing trustworthy classification methods. This method worked effectively in Instant Social Networking (ISN) between communicating-ends trust establishment (Yan *et al.,* 2014).

Therefore, all mentioned findings emphasized mostly on ensuring data transmissions and authentications trust; however, they do not show data integrity and control of the cloud storage provider level (side). Considering data protection and security at cloud data centers level, the cryptographic concept is proposed (Plantard *et al.,* 2013). Nevertheless, the current security solutions on cloud storage base on regulatory compliance methods i.e. the service level agreement (SLA) to limit cloud users (providers or consumers) reputations (Modi *et al.,* 2013). Hence, the data leakage is resolved by employing cryptography algorithms only. As a result, based on current results and data security issues, organizations are unable to overcome the current attack activities due to fact that they are under upgraded and unreliable cryptographic algorithms.

In this paper, we propose secure and reliable cloud storage architecture with robust data security measures based on the hardware level. The use of TPM to store confidential data (short in size) guarantees its (data) security, availability (in case of need), and confidentiality; because it is impossible to manipulate the TPM's information as a result of PCR registers that stores encrypted data that can only be decrypted by the same TPM attached to the single hardware component on the architecture Microsoft (2017). In addition to that, it is not transferable, i.e., it cannot be transferred from one user to another for further manipulations.

Materials and Methods

In this section, we describe our approach with respect to architecture displayed in Figure 1. Data D is encrypted first and then segmented into two or more (based on your settings) encrypted data blocks (D1 and D2), and later distribute them to different cloud data centers (DC1 and DC2 or more). The segmented data is composed of characters (ciphertext) that has a fixed size per block. This data block contains data (ciphertext) and block ID. Using character data type will help the user to know whether his/her data is still as it was during decryption and merge processes. The HBS is presented to eliminate cloud data leakages from internal or external attacks reliably. Since the keys required for encryption and decryption are generated and used by the TPM itself, this paper does not detail much on the private and public key creation and usability.

Definition 1 HBS Let D be considered as initial user data and DC1 and DC2 be cloud data centers. From here, we can derive a secure method to store in the cloud data centers effectively with no data leakages whether internally or externally attack. The supplied initial data D is composed of user data to be stored in the cloud storage (DC). The derived values from D1 and D2 are two separate encrypted data blocks to be distributed across different cloud data centers (DCs). In addition, while evoking encryption and decryption functions from the user side, the encryption, and decryption keys must remain stored in the TPM registers (the Platform Configuration Registers/ PCR). Given that an adversary from internal or external attack gains access to a single encrypted data block (D_i) stored in a certain datacenter DC_i, he will need all blocks (of encrypted data) as well as a decryption key to access meaningful information. Based on our HBS architecture which is built on TPM capabilities, he will never succeed because none can penetrate TPM registers even if it (TPM) is detached from the

user's unit. Moreover, encryption and decryption operations are taken within the TPM, hence keys used with both operations never leave the TPM PCR (Emmy *et al.,* 2018).

A Secure Efficient Data Distribution Model

This Secure Efficient Data Distribution (SEDD) model is composed of Data Distribution Process (DDP) function. This function is used to protect data from unexpected attack from both users and cloud service provider's employees. Figure 2 shows a high-level DDP workflow structure in SEDD model. This figure exemplifies the principle of our approach mechanism.

As mentioned earlier, we present two steps in this model (displayed on the left and right frames in the figure). These steps constitute other important procedures taken while transferring/accessing data to/from the cloud data centers. At first, it constitutes a data processing procedure that allows data segmentation (user data) as the input of two distinct data blocks. Second, it merges the two segments (data blocks) to retrieve the original data from the cloud data centers.

At the first step, we segment the input data D into two distinct blocks D1 and D2 followed by encryption computation respectively, as shown in Figure 2. Moreover, to accomplish encryption process, we generate a random parameter data E to calculate new data block X by computing D - E. Furthermore, an encryption key K is fetched from a TPM register planted on the user's PC (side). This key K is used to compute an XOR operation of E and X. The key K will never leave the TPM's PCR and it is known by TPM chip at the user' side only. In addition to that, the cloud providers have rights to know what is stored or outsourced to their storage facilities regarding user's date. Secure data distribution is articulated since keys are stored in a hardware level. Hence, encrypted data blocks are distributed to cloud data centers.

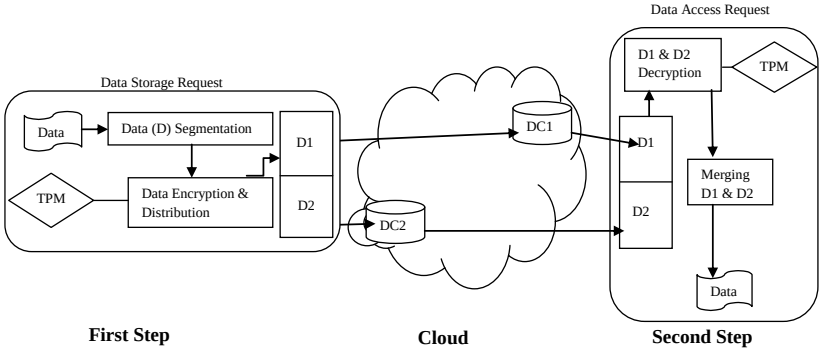

Figure 2. DDP workflow structure in SEDD model

In the second step, we model how the user retrieves Data (D1 and D2) from the cloud. From here, to access the original data from cloud data centers, the received data segments are decrypted using key K (stored on user's TPM) which is applied to XOR operations on both data segments. Moreover, the decrypted data segments need to be merged together to produce the original user data D.

Attacker Challenger Models

The cloud storage serves as a trustable resource in cloud service deployment models, whereby cloud service model designers consider the cloud service providers trusted and reliable. Nevertheless, a number of risks are stimulated by unexpected service provider's behaviors instead of the external attacks. This becomes a moral instead of a technical consequence in many cases, since cloud providers often require to access the user data for the purpose of data governance; which is against cloud regulations and Service Level Agreements (SLA). Therefore, data become insecure albeit encryption techniques have been applied. In this perspective, we assume that the prior attack may come from the cloud provider and user levels (sides), and we define two attacker challenge models with regard to the current cloud practices.

SLA attack (SA) Model; here, cloud providers are considered to be the source of data attack with no compliance with cloud regulations and SLA. Cloud service providers are considered to have full access to the cloud data centers and the cryptographic keys.

Adversary attack (AA) Model; we consider both internal and external attackers with successful access to the data and arrive at basic background information. When these adversaries have basic knowledge of the data stored in the cloud, they will try to guess the encrypted information.

The definition of this attacker challenge models are described below;

Definition 2 SLA attack model for a key K to decrypt a data D from the cloud, as $K \rightarrow D$. Consider that cloud adversaries use key K to access data D with no authorization from the owner.

Results

SEDD Algorithms This section describes the proposed algorithms. There are two primary algorithms that implement the security model, which include Secure Data Distribution (SDD) and Data Retrieval (DR) algorithms.

Secure Data Distribution Algorithm

This algorithm implements the data processing before it is outsourced to the cloud data centers. It accomplishes the First Step in the SEDD model as demonstrated in Figure 2. First, the supplied initial inputs of SDD include the user Data (D), a randomly generated parameter E with a cryptographic TPM key K. The end result of this algorithm consists of two distinct encrypted data blocks D1 and D2. The significance of this algorithm can guard or defeat the attack challenge models. For instance, in the SA attack model, we consider cloud providers to have the Key K that can allow them to access the data (user data) from the cloud datacenter. From here, the cloud providers (staffs) will not sufficiently access full information required to construct the original data from two distinct cloud data centers. The AA attack model considers both internal and external adversaries with basic knowledge of stored data. Unfortunately, if the adversary tries the malicious attack on the data, they will be defeated as attackers in the SA model. Therefore, our approach can guarantee effective defense against both attack challenge models. The SDD algorithm is given in Algorithm 1.

Variable: D, E, D1, D2, Result, X, K
1: Supply D, E, K
2: Init X ← 0; D1 ← 0; D2 ← 0
3: Randomly generate E < D value
4: Fetch key K from TPM
5: **For All** D **Do**
6: **If** D ≠ E **&&** E ≠ 0 **then**
7: **Do** X ← D – E
8: D1 ← E⊕K
9: D2 ← X⊕K
10: **End If**
11: **End For**
12: Result D1, D2

Algorithm 1 Secure Data Distribution (SDD)

Data Retrieval Algorithm

Data retrieval (DR) algorithm allows users to access the original data from the cloud data centers by decrypting and merge two data blocks. This is described in Figure 2 as Second Step. DR's initial data inputs are two distinct data blocks D1 and D2 identified by their IDs (this ID is present in every data block as its unique identification in every situation) from cloud data centers and a key K from TPM chip (on user' side). Data block D1 and D2 must be present in the data center DC1

and DC2 before merge process, and their availability determines the time (slow or fast) taken to complete the data D retrieval; since, DC1 and DC2 response varies (not equal) independently. The DR result is the original data D. It is proved original during merge process by checking the data block size and its IDs. Given that; the size and IDs are not compatible with the known fixed size and IDs set at the time of distribution process, the merge process will not succeed. The following is DR Algorithm 2.

Variable: D1, D2, K, D, A, Result
1: Supply D1, D2, K
2: Init A ← 0; B ← 0; D ← 0
3: Fetch key K from TPM
4: A ← D1⊕K
5: B ← D2⊕K
6: D ← A + B
7: Result D

Algorithm 2 Data Retrieval (DR)

Discussion: HSB Evaluation

To evaluate the HSB performance metrics, we look at the time required while distributing and retrieving data to/from the cloud data centers, with regard to different supplied size of the data. To establish the cloud environment, we employed the Cloud platform on Ubuntu Linux 14.04 Operating System for cloud computing development and simulation. A Lenovo (former IBM) computer operating on Inter (R) Core (TM) i5-3230M, 2.60GHz and 8.00GB RAM was used with TPM emulated API from MIT project on a Local Area Network (LAN). Figure 3 shows the increase in time with respect to the size of the data during SDD processes.

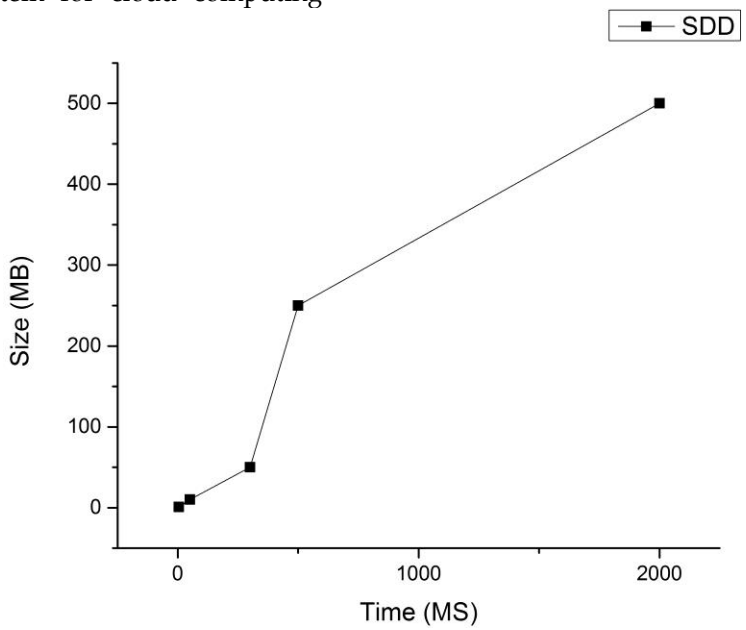

Figure 3. SDD performance evaluation

The results show that SDD processing time increased with the increase in the size of the data. We consider the time taken to fetch encryption key K from TPM, data (D) encryption and segmentation processes, and data (D1 and D2) distribution process. The size of the data determines the performance metrics of the SDD algorithm in our SEDD model.

For the data retrieval (DR) evaluation, Figure 4 shows that the performance time required for DR is longer compared to SDD with the same data size.

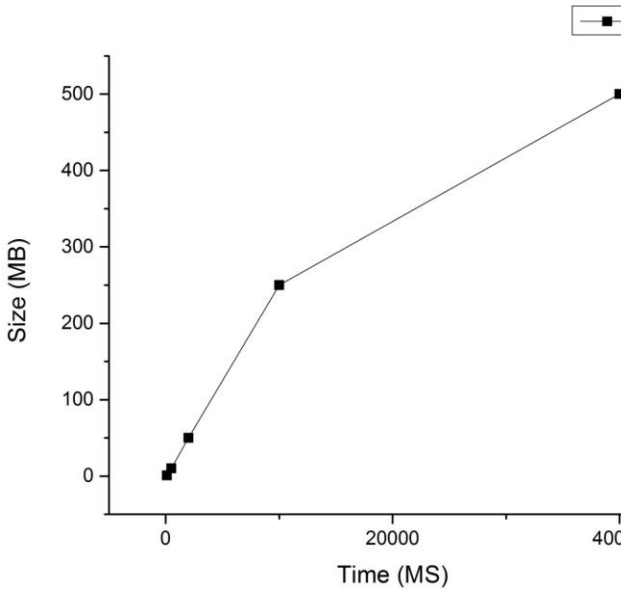

Figure 4 DR performance evaluation

The evaluation takes into account the time required to retrieve data blocks (D1 and D2) from the data centers (DC1 and DC2), fetching decryption key K from the TPM, decryption and merging processes. Therefore, the size of the data and its retrieval process determines the performance metrics of the RD algorithm in the SEDD model.

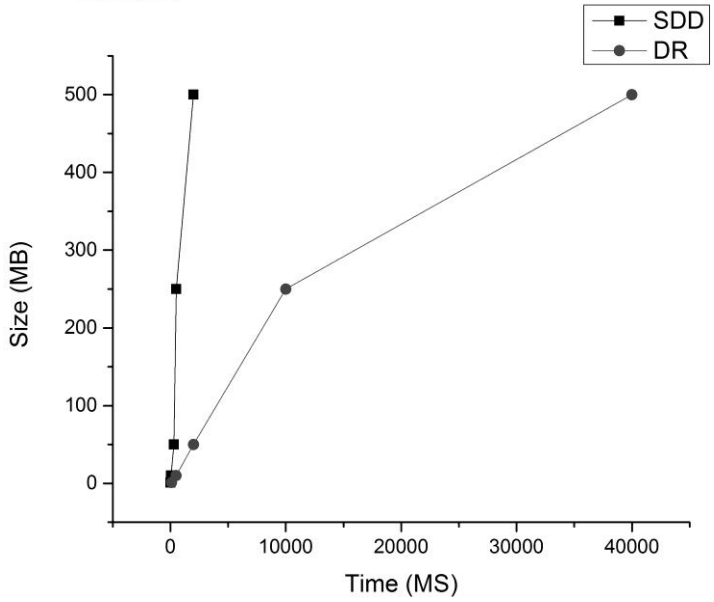

Figure 5. Comparison between SDD and DR performance evaluation

Figure 5 illustrates the comparison between SDD and DR performance evaluation. Consequently, SDD performance time required to distribute the data differ much far compared to DR's. For DR, the performance is based on data center response time required to release the data blocks (D1 and D2) for decryption process at the initial stage of DR. This shows that the faster the data center, the faster the DR algorithm is. For SDD, the time required is less due to its fewer computation operations than DR. In terms of HSB scalability, the HSB is scalable due to the fact that TPM capabilities can be detached or implemented from/to existing hardware TPM defined (scale down) or new hardware TPM defined (scale up) component. The implementation or removal of TPM capabilities to/from hardware component of the HSB architecture demonstrates the scalability aspect of the system in general scenario.

Conclusion

This work tends to eliminate security and inefficient performance issues of the cloud data storage based on HSB architecture. It models the approach that prevents the cloud from internal and external attack to access the data (user data).

Therefore, a Secure Efficient Data Distribution (SEDD) model is presented. In this model, we implemented two algorithms, i.e. Secure Data Distribution (SDD) and Data Retrieval (DR) algorithms. The performance evaluation, results show that the proposed approach can effectively defeat cloud internal and external attackers from unauthorized access to the original data (user data). The time required for SDD and DR depends on the size of the data and datacenter's response time respectively, since response time may be interrupted by internet connection variations from both (request and response sources) and size (not fixed and varies) of the data in the request packet or to/from download from the datacenter.

There is less literature in our region concerning trusted computing in the field of data security. Therefore, there is a need to further study data security and storage along regional premises (cloud infrastructure) in the future for EAC sustainable resilience.

References

Ali, M., Khan, S., Vasilakos, A. (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, pp. 357–383.

EAC. (2019). ICT4Business. https://www.eac.int/press-releases/150-infrastructure/1528-ict4business-brings-together-rwandese-industry-and-cenit-ea-to-shape-the-digital-transformation. Kigali, Rwanda

Cao, N., Wang, C., Li, M., Ren, K., Lou, W. (2014). Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Transactions on Parallel Distributed Systems, 25, pp. 222–233.

Centre for the Protection of National Infrastructure, (2010), "Information Security Briefing 01/2010 Cloud Computing", http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf

Chang, V., & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. IEEE Transactions on Service Computing, 9, pp. 138–15.

Chen, C., Zhang, C. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on big data. Information Sciences, 275, pp. 314–347.

Cimino, M., & Marcelloni, F. (2011). Autonomic tracing of production processes with mobile and agent-based computing. Information Sciences, 181, pp. 935–953.

Cloud Security Alliance, (2010), "Top Threats to Cloud Computing V1.0", https://cloudsecurityalliance.org/research/top-threats

Cloud Security Alliance, (2011), "Security guidance for critical areas of focus in Cloud Computing V3.0", https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Costa, K., Pereira, L., Nakamura, R., Pereira, C., Papa, J., Falcão, A. (2015). A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks. Information Sciences, 294, pp. 95–108.

Darrell, L. (2015). Unlimited cloud storage at amazon.com. The Bidnessetc (http://www.bidnessetc.com/58232-nlimited-cloud-storage-at-amazoncom-inc- on- black- friday/).

Emmy, M., Zhang, G. (2018). "A Reliable Secure Storage Cloud and Data Migration Based on Erasure Code", KSII Transactions on Internet and Information Systems. Vol. 12, NO. 1, 2018. DOI: 10.3837/tiis.2018.01.021

Gai, K., Qiu, L., Zhao, H., Qiu, M. (2016). Cost-aware multimedia data allocation for heterogeneous memory using genetic algorithm in cloud computing. IEEE Transactions on Cloud Computing, 1, pp. 99.

Gai, K., Qiu, M., Chen, L., Liu, M. (2015). Electronic health record error prevention approach using ontology in big data. 17th IEEE International Conference on High Performance Computing and Communications. New York, USA, pp. 752–757.

Gai, K., Qiu, M., Thuraisingham, B., Tao, L. (2015). Proactive attribute-based secure data schema for mobile cloud in financial industry. The IEEE International Symposium on Big Data Security on Cloud. IEEE 17th International Conference on High Performance Computing and Communications. New York, USA, pp. 1332–1337.

Gai, K., Qiu, M., Zhao, H., Tao, L., Zong, Z. (2015). Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. Journal of Network Computer Application. 59, pp. 46–54.

Gartner Inc, (2011), "Gartner identifies the Top 10 strategic technologies for 2011", http://www.gartner.com/it/page.jsp?id=1454221

Howley, D., (2015). Microsoft's one-drive the best cloud storage service? The Yahoo (https://www.yahoo.com/tech/microsoft- kills- unlimited- onedrive- accounts-1759 27221.html).

United Nations, (2013). Information Economy Report. United Nations Conference on trade and development, https://unctad.org/system/files/official-document/ier2013_en.pdf, New York, Geneva

Khalid, A. (2010), "Cloud Computing: applying issues in Small Business", International Conference on Signal Acquisition and Processing (ICSAP'10), pp 278–281

KPMG, (2010), "From hype to future: KPMG's 2010 Cloud Computing survey", http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs-2010-cloud-computing-survey/2384291

Li, M., Yu, S., Zheng, Y., Ren, K., Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel Distributed Systems, 24, pp. 131–143.

Liu, Q., Wang, G., Wu, J., (2014). Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Information Sciences, 258, pp. 355–370.

Liu, S., Qu, Q., Chen, L., Ni, L. (2015). SMC: A practical schema for privacy-preserved data sharing over distributed data streams. IEEE Transactions on Big Data, 1, pp. 68–81.

Microsoft. (2021). Trusted Platform Module Technology Overview. https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview

Microsoft. (2017). Understanding PCR banks on TPM 2.0 devices. https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/switch-pcr-banks-on-tpm-2-0-devices

Marinos, A. & Briscoe, G. (2009), "Community Cloud Computing", In 1st International Conference on Cloud Computing (CloudCom), Beijing, China, Springer-Verlag Berlin, Heidelberg

Mather, T., Kumaraswamy, S. & Latif, S. (2009), "Cloud Security and Privacy", O'Reilly Media, Inc., Sebastopol, CA

Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M (2013) A survey on security issues and solutions at different layers of cloud computing. Journal of Supercomputers. 63, pp. 561–592.

Pedrycz, W. (2014). Allocation of information granularity in optimization and decision-making models: Towards building the foundations of granular computing. European Journal of Operation Research, 232, pp. 137–145.

Plantard, T., Susilo, W., Zhang, Z. (2013). Fully homomorphic encryption using hidden ideal lattice. IEEE Transaction on Information Forensics Security, 8, pp. 2127–2137.

Popovic, K. & Hocenski, Z. (2010), "Cloud Computing Security issues and challenges", In Proceedings of the 33rd International convention MIPRO", IEEE Computer Society, Washington DC, USA, pp 344–349

Times Reporter, (2012). EAC cloud sourcing summit. The New Times. https://www.newtimes.co.rw/section/read/56424, Nairobi Kenya

Qiu, M., Gai, K., Thuraisingham, B., Tao, L., Zhao, H. (2016). Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. Future Generation of Computer Systems, 1.

Qiu, M., Zhong, M., Li, J., Gai, K., Zong, Z. (2015). Phase-change memory optimization for green cloud with genetic algorithm. IEEE Transactions on Computers, 64, pp. 3528–3540.

Rosado, D.G., Gómez, R., Mellado, D. & Fernández-Medina, E. (2012), "Security analysis in the migration to cloud environments", Future Internet, Vol. 4, pp. 469–487

Song, T., Pan, L., Paun, G. (2013). Asynchronous spiking neural P systems with local synchronization. Information Sciences, 219, pp. 197–207.

Wang, C., Chow, S., Wang, Q., Ren, K., Lou, W. (2013). Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on Computers, 62, pp. 362–375.

Wu, G., Zhang, H., Qiu, M., Ming, Z., Li, J., Qin, X. (2013). A decentralized approach for mining event correlations in distributed system monitoring. Journal of Parallel Distributed Computing, 73, pp. 330–340.

Yan, Z., Chen, Y., Shen, Y. (2013). A practical reputation system for pervasive social chatting. Journal of Computer Systems Science, 79, pp. 556–572.

Yan, Z., Wang, M., Zhang, P. (2014). A scheme to secure instant community data access based on trust and contexts. in: IEEE International Conference on Computer and Information Technology. IEEE. Xi'an, China, pp. 646–651.

Yan, Z., Zhang, P., Vasilakos, A. (2014). A survey on trust management for internet of things. Journal of Network Computer Applications, 42, pp. 120–134.

Yu, K., Gao, Y., Zhang, P., Qiu, M. (2015). Design and architecture of dell acceleration appliances for database (DAAD): A practical approach with high availability guaranteed. IEEE 17th International Conference on High Performance Computing and Communications, IEEE, pp. 430–435.

Zhang, S., Zhang, S., Chen, X. & Huo, X. (2010), "Cloud Computing Research and Development Trend", In Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China, IEEE Computer Society, Washington, DC, USA, pp 93–97.

Zhao, G., Liu, J., Tang, Y., Sun, W., Zhang, F., Ye, X. & Tang, N. (2009), "Cloud Computing: A Statistics Aspect of Tenants", In First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp 347–358.