Security and Privacy Challenges in Cloud Computing: A Review

Miss. Sayali Karmode Yelpale

Assistant Professor (CS & IT) at Satish Pradhan Dnyanasadhana College, Thane

sayalis.karmode@gmail.com

Abstract

Cloud computing is being transformed into a model with services. It is mainly focused on the concept of dynamic provisioning, which is applied to services as well as to the capacity, storage, networking, and information technology infrastructure. This paper reviews the key concepts of cloud computing exist. We are presenting here various concepts of cloud computing. According to the previous few surveys we are presenting various security challenges and for that what solution are overcome.

Keywords*:* Cloud computing, Virtualization, Security, Privacy, Data protection.

1.Introduction

Cloud computing is the availability of computer system resources, especially data storage (cloud storage) and computing power, without computer direct active management. The term is commonly used to describe the data centers available to most users of the Internet. The most widely used definition of the cloud computing model is NIST [1] "a model for enabling network access on-demand, which corresponds to a shared pool of configurable resources (eg networks, servers, storage, applications, and services). Its main features are cloud model multitenancy and elasticity. Multi-tenancy enables sharing of a single service example.Sensitive information in the context of cloud computing contains data from different fields and categories. Health data is an example of sensitive

Received: April 2, 2020 Revised: May 27, 2020 Accepted: June 25, 2020

DOI: 10.5281/zenodo.3909981

information being managed in a cloud computing environment, and many want to keep health-related information safe. Therefore, in recent years, the proliferation, privacy and data security requirements of these new cloud technologies have been developed to protect individuals from surveillance and database exposure. Some examples of such protection legislation are the EU Data Protection Directive (DPD) [2] and the US Health Insurance Portability and Accountability Act (HIPAA), which require privacy protection to maintain personally identifiable information. This paper presents an overview of research on the security and confidentiality of sensitive data in cloud computing environments.

We have seen new developments in the cloud provider orchestration, resource control, physical hardware, and cloud service management layers. We also conduct sophisticated reviews of sensitive data systems, such as sophisticated threat modeling, privacy enhancement protocols, and solutions for managing sensitive data in cloud computing. The rest of this paper is organized as follows. Section 2 provides an overview of cloud computing concepts and technologies. Section 3 describes the security and privacy issues that need to be addressed to provide secure data management for cloud environments. Section 4 reviews current security solutions in the field of cloud computing. Section 5 describes research on privacy protection solutions for sensitive data. Finally, in Section 6, we present our conclusions.

2. Key Concepts

Over the years, major IT vendors (such as Amazon, Microsoft, and Google) have been offering virtual machines (VMs) for their customers to rent. These clouds use hardware sources with dynamic load balancing and on-demand provisioning and support direct migration of the VM. By providing VM through the cloud, the company's entire datacenter footprint can be reduced from thousands of physical servers to hundreds (or even dozens) of hosts. Although cloud computing is practical and costs effective in this way, security can be a problem when using non-home systems.

Many concepts and techniques are widely used in cloud computing, including virtualization mechanisms, types of cloud services, and "container" methods for finding optimal solutions.Virtualization System Hypervisor or Virtual Machine Monitor (VMM) is an important part of VM and hardware life for managing virtualized resources. It provides a way to run multiple standalone virtual machines on the same physical host. Hypervisors can be divided into two groups:

Type I hypervisor

The Type I hypervisor works directly on the host's hardware, known as bare metal, to monitor hardware and guest virtual machines. Generally, they don't need pre-installed software. Instead, you can install it on the appropriate hardware. This type of hypervisor is powerful and requires many skills to perform well. Additionally, Type I hypervisors are more complex and require some hardware to function properly. For this reason, IT operations and data center computing is a top priority.
Examples of Type I hypervisors are XP Oracle VM Server, Spark, Oracle VM Server for X86, Micro .ft Hyper-V, and ESM / ESX of VMware.

Type II hypervisor

Received: April 2, 2020 Revised: May 27, 2020 Accepted: June 25, 2020

DOI: 10.5281/zenodo.3909981

It is also called host hypervisor because it is installed on most common operating systems. They cannot do more complex virtual tasks. People use it for basic development, testing, and simulation. If a security error is detected on the host OS, it compromises all running virtual machines. Therefore, Type II hypervisors cannot be used for data center computing. They are designed for low-end end-user systems. For example, developers can use Type II hypervisors to enable virtual machines to test software products before they are released.Virtual B, X, VMware Workstation, and Fusion are a few examples.

2.1 Cloud Model

Even though distributed computing has advanced over the time it has been significantly partitioned into three wide help classes: Infrastructure as a Service(IAAS), Platform as a Service (PAAS) and Software as a Service (SAAS) which are extensively examined underneath:

2.1.1 IaaS. (Infrastructure as a Service)

IaaS low-level cloud service model. With IaaS, users are provided with preconfigured hardware resources through a virtual interface. Unlike PaaS and SaaS, IaaS does not include application or non-operating operating systems (all left to the customer), which extends to the infrastructure needed to support or support the software support. IaaS Corporate Data Backup is only available for company website servers with network bandwidth or for those with previous supercomputers, providing additional storage to enable access to high-power computing. Popular IaaS interfaces, such as Amazon EC2, IBM Software, and Google's Compute Engine (GCE), silently trigger the Internet, whether consumers want it or not.

2.1.2 PaaS (Platform as a Service)

PaaS is a cloud service model that provides users with a platform to develop, launch, and manage applications. PaaS offerings usually include a basic operating system, application, and development tools. PaaS eliminates the need for organizations to build and maintain traditionally used architectures to develop applications. The pass is sometimes referred to as 'middleware', which in theory means sitting somewhere else.

2.1.3 SaaS (Software as a Service)

Sometimes referred to as an on-demand software model, SaaS is a software licensing and delivery model where a fully functioning and full-fledged software product is distributed to users on the web on a subscription basis. SaaS offers are usually accessed by end-users through a web browser (which greatly disrupts the user's operating system) and can be charged monthly or more depending on usage. SaaS offers are the most common of all cloud computing service models. Many consumers use SaaS products without detection. Popular products such as Office 365 and Salesforce are leading SaaS offerings in the workplace and are used by thousands of businesses every day.

The NIST Cloud Computing Reference Architecture [7] defines five key actors in the cloud arena: cloud customers, cloud providers, cloud carriers, cloud auditors, and cloud brokers. Each of these

Received: April 2, 2020 Revised: May 27, 2020 Accepted: June 25, 2020

DOI: 10.5281/zenodo.3909981

actors is a company (an individual or organization) that engages in a cloud computing transaction or process and/or performs cloud computing work. Cloud Customer is a person or organization that uses services from cloud providers in the context of business relationships. Cloud Provider is a company that provides cloud services to interested customers. The Cloud Auditor performs an independent assessment of cloud services, functions, performance, and security about cloud deployment. A cloud broker that manages the use, performance and delivery of cloud services establishes relationships between cloud providers and cloud customers.

Cloud Carrier is a company that provides connectivity and transport of cloud services from cloud providers to cloud customers via physical networks. Cloud providers' activities can be classified into five main categories: service deployment, resource acquisition, physical resources, service management, security, and privacy. Service deployment means providing cloud users with one of the service models (SaaS, PaaS, IaaS). Resource extraction is the provision of interfaces to interact with networking, storage, and computing resources.

The physical resources layer includes facilities available through the physical hardware and resource abstraction layer. Service management includes providing business support, resource allocation, configuration management, portability, and interoperability to other cloud providers or brokers. Integrating solutions to legally deliver cloud services to cloud users covers the security and privacy obligations of cloud providers.

2.2 Containers

Holders offer a coherent bundling system where applications can be preoccupied with the earth in which they run. This decoupling permits compartment based applications to be sent effectively and reliably, whether or not the objective condition is a private server farm, the open cloud, or even a designer's PC. Containerization gives a spotless detachment of worries, as engineers center around their application rationale and conditions, while IT activities groups can concentrate on sending and the board without wasting time with application subtleties, for example, explicit programming renditions and setups explicit to the app[8]. LXC advancements were presented during the 1980s, beginning with the chroot (change root) order and develop into well-known compartment chiefs, for example, Docker.

• Chroot, the Unix chroot framework call, which was presented as a component of Unix variant 7 out of 1979, can be considered as the initial phase in the advancement of containerization. The chroot considers changes the root index of the calling procedure to a predefined way, where the root registry is known by all offspring of the calling process[9]. This element is utilized by certain holders for detachment and sharing the hidden document framework. Chroot is regularly utilized when building framework pictures by changing root to a brief index, downloading and introducing bundles in chroot, or compacting chroot as a framework root record framework.

• FreeBSD Jail7 stretched out chroot in 1998 to give improved security. FreeBSD prison settings can expressly confine access outside the sandbox condition by documents, procedures, and client accounts (counting accounts made by the prison definition). Prison can, along these lines, characterize another root client, who has full control inside the sandbox, yet who can't arrive at anything outside[10].

• Namespaces were presented in 1992 [11] for process-based asset separation. Namespaces give apparatuses to disengaging the perspective on worldwide assets, for example, insights regarding document frameworks, forms, arrange interfaces, Inter-Process Communication (IPC), hostnames, and

Received: April 2, 2020 Revised: May 27, 2020 Accepted: June 25, 2020

DOI: 10.5281/zenodo.3909981

client IDs. Procedures in a specific namespace are imperceptible to different procedures since they imagine that they are the main procedures on the framework and because "availability" is just allowed with the parent namespace.

• Linux Security Modules (LSMs) are part modules that give a structure to required access control (MAC) security usage. In MAC usage, the chairman (client or procedure) allots get to controls to the subject/initiator. An optional access control (DAC), the asset proprietor (client) doles out access controls to the subject or initiator. Existing LSM executions incorporate AppArmor, SELinux, etc to keep virtual machines from assaulting other virtual machines or the host. For this reason, strategies are utilized to characterize what activities a procedure can perform on a specific framework.

Each framework incorporates a worldwide zone for both framework and framework wide authoritative control and may have at least one non-worldwide zones. All procedures run in the worldwide zone if there is no non-worldwide zone. The worldwide zone knows about all gadgets and all record frameworks, while non-worldwide zones don't know about the presence of some other zones. Zone-based holders give disengagement, security, and virtualization. Zones are like correctional facilities with extra highlights, for example, depictions and cloning that cause it is conceivable to clone effectively to or to copy a current zone into another zone[12]. In 2005 OpenVZ 9 holders were presented utilizing an adjusted Linux part with a lot of augmentations. OpenVZ depends on the namespace and control bunch ideas as opposed to prisons, which were utilized in FreeBSD. Later in 2008, LXC10 developed as a compartment the executive's instrument and its joined namespaces and control gatherings to make a completely disengaged condition. It gives libraries and order line backing to empower directors to make new compartments. LXC compartments can be utilized in either favored (as a root client) or unprivileged (as a non-root client) modes to effortlessly tweak bit abilities or design gatherings to fulfill the specific prerequisites.

Docker is another holder of the executive's device – it was presented in 2013 and depends on namespaces and SELinux. Docker gives robotization to the organization of holders through remote APIs and has extra highlights that make it conceivable to make normalized conditions for creating applications. This has made Docker a mainstream innovation. Making normalized conditions is accomplished utilizing a layered picture design that empowers clients to include or expel applications and their conditions to frame a confided in the picture. Docker pictures can run unaltered on any stage that bolsters Docker. In Docker, holders can be made from manufacturing documents, for example, Web administration the board. The utilization of holders in distributed computing is progressively getting well known among cloud suppliers, for example, Google11 and Microsoft12. Noteworthy upgrades in execution and security are the principle driving components for utilizing holders contrasted with virtualization utilizing hypervisors in cloud infrastructures[13].

3. Security Challenges

There are several key components to security in any infrastructure—and the cloud is no exception. They are as follows:

3.1 Multitenancy

Received: April 2, 2020 Revised: May 27, 2020 Accepted: June 25, 2020

DOI: 10.5281/zenodo.3909981

Multitenancy is the point at which a few distinctive cloud clients are getting to similar processing assets, for example, when a few unique organizations are putting away information on the equivalent physical server, nonetheless, the sharing of assets implies that it tends to be simpler for an aggressor to access the objective's information.

3.2 Loss of control

Loss of control happens when customers lose their power over their assets in the hand of a specialist co-op. As an absence of validation and access control put by suppliers, loss of control adds to more prominent security concerns. As the clients don't have express power over their information, this makes it feasible for cloud suppliers to perform information mining over the clients' information, which can prompt security issues. Additionally, when the cloud suppliers reinforce information at various server farms, the purchasers can't be certain that their information is eradicated wherever when they erase their information. This can prompt abuse of the unerased information. In these kinds of circumstances where the customers lose authority over their information, they consider them to be a supplier as a black-box where they can't legitimately screen the assets transparently[14].

3.3 Trust Chain in Clouds:

Trust assumes a significant job in pulling in more shoppers by guaranteeing cloud suppliers. Because of loss of control (as examined prior), cloud clients depend on the cloud suppliers utilizing trust systems as an option in contrast to giving clients straightforward command over their information and cloud assets. Accordingly, cloud suppliers manufacture certainty among their clients by guaranteeing them that the supplier's activities are ensured consistent with hierarchical protections and guidelines.

4. Security solutions

4.1 Identity and Access Management

The vital functionalities of identity management systems for the success of clouds concerning shopper satisfaction. The authors conjointly gift Associate in Nursing authorization system for cloud federation victimization Shibboleth - an ASCII text file implementation of the safety assertion language (SAML) for single sign-on with totally different cloud suppliers. This resolution demonstrates however organizations will source authentication and authorization to 3rd party clouds victimization an identity management system. Stihler et al. [15] conjointly propose integral united identity management for cloud computing.

In [16], the authors take into account the problems relating to the inter-cloud federation and also the projected ICEMAN identity management design. ICEMAN discusses the identity life cycle, self-service, key management, provisioning, Associate in Nursingd provisioning functionalities that require to be enclosed in an applicable intercloud identity management system. The EGI delivered a hybrid united cloud as a collaboration of communities developing, innovating, operating, and victimization clouds for analysis and education. The EGI united cloud provides IaaS, persistent block storage connected to VMs, and object-level storage for clear information sharing. The EGI controls access to

Received: April 2, 2020 Revised: May 27, 2020 Accepted: June 25, 2020

DOI: 10.5281/zenodo.3909981

resources victimization X.509 certificates and also the thought of "Virtual Organization" (VO). VO refers to a dynamic set of users or establishments victimization resource sharing rules and conditions[16].

4.2 Confidentiality, Integrity, and Availability

Santos et al. [17] extend the Terra [18] style that allows users to verify the integrity of VMs within the cloud. The projected resolution is named the trusty cloud computing platform (TCCP), and therefore the whole IaaS is taken into account to be one system rather than granular hosts in Terra. during this approach, all nodes run a trusty virtual machine monitor to isolate and shield virtual machines. Users are given access to cloud services through the cloud manager part. The external trusty entity (ETE) is another part that gives a trust organizer service to stay track of the trusted VMs in an exceeding cluster. The ETE is often wont to attest to the protection of the VMs. A TCCP guarantees confidentiality and integrity in knowledge and computation and it additionally allows users to attest to the cloud service supplier to make sure whether or not the services are secure before putting in place their VMs. These options are supported by the trusty platform module (TPM) chip. The TPM contains a non-public endorsement key that unambiguously identifies the TPM and a few cryptologic functions that can't be altered.

Fuzzy authorization (FA) for cloud storage is another versatile and ascendible approach to change knowledge to be shared firmly among cloud participants. solfa syllable ensures confidentiality, integrity, and secure access management by utilizing secret sharing schemes for users with smartphones who are mistreatment cloud services.

In [19] the authors advise swap and play as a new technique for remain updating of hypervisors without the prefer to reboot the VM for excessive availability. The proposed plan is scalable, usable, and applicable in cloud environments and it is been carried out in Xen as one of the most famous hypervisors. Change and play furnish strategies to swap the in-reminiscence country of the on-foot hypervisor to the updating nation, in a similar fashion to updating the underlying host. Swap and play embody three independent stages: practice, distribution, and replacement. Inside the practice section records for the later country, the switch is gathered. The distribution section deploys the replace bundle deal on the goal host for updating. Inside the remaining step, the replace bundle is patched to man or female hosts in the cloud. Every host applies the replace bundle to deal independently of the others and does no longer requires any community resources. The Xen implementation of the trade and play reply is recognized as swapvisor. Swapvisor introduces a manufacturer's new hypercall internal to the Xen structure. A hypercall is a entice from a website to the hypervisor (just like a syscall from a utility to the kernel). Hypercalls are used via domains to request privileged operations collectively with updating web page tables. The experiments exhibit that updating from Xen mannequin four. two zero to mannequin four. two 1 is fulfilled inside about forty 5 ms which looks to be intangible and has nearly zero affect the neighborhood performance.

Klein et al. [19] decorate cloud business enterprise resilience the utilization of a load-balancing mechanism seemed like brownout. The questioning in the again of this reply is to maximize the optional contents to offer a solution this is resilient to volatility in terms of flash crowds and possible shortages (thru load balancing over replicas) while in evaluation to distinctive strategies which may be implemented the usage of response-time or queue length. In any unique attempt [20] the authors proposed a synchronization mechanism for cloud accounting systems that can be distributed. The run-

Received: April 2, 2020 Revised: May 27, 2020 Accepted: June 25, 2020

DOI: 10.5281/zenodo.3909981

time resource utilization generated from awesome clusters is synchronized to preserve a cloud-huge view of the information simply so a single bill may additionally be created. The authors additionally proposed a hard and fast accounting tool requirements and an evaluation approach that verifies that the respond fulfills those necessities.

4.3 Authentication and authorization

Fermicloud [20] uses any other method for authentication and authorization - it makes use of public key infrastructure (PKI) x. 509 certificates for customer identity and authentication. Fermicloud is built-in opennebula117 and it develops every x. 509 authentication in sunstone open nebula – a web interface meant for patron administration – and x. 509 authentication by using command-line interfaces. To avoid the barriers of open nebula get entry to governing lists which are used for authorization after worthwhile authentication of users, authors built-in a present close by credential mapping carrier. This answer has additionally been extended in cloud federations to authorize customers during unique cloud carriers which have set up trust relationships through relied on certification government.

Integrating agree with cryptographic position-primarily based access manage (RBAC) [21] is every other answer that ensures believe for the comfy sharing of statistics inside the cloud. The authors advise using cryptographic RBAC to put into effect authorization rules regarding the trustworthiness of roles that are evaluated with the aid of the information owner. One other characteristic of the authorization machine in this answer is that it develops a brand new concept using role inheritance for comparing the trustworthiness of the gadget. In any other examination, sendo et al. [21] endorse a consumer-centric approach for platform-degree authorization of cloud offerings the use of the oauth2 protocol to allow services to act on behalf of users when interacting with other offerings to avoid sharing usernames and passwords across the provider.

5. Privacy-preservation for sensitive data in cloud computing

Outsourcing privateness is every different situation remember that is mentioned in [21]. The authors define the thinking of "outsourcing privacy" the place a database proprietor updates the database greater time on untrusted servers. This definition assumes that database consumers and the untrusted servers are not successful to learn about some elements about the contents of the databases barring approved get proper of entry to. The authors implement a server-side indexing form to produce a system that lets in a single database proprietor to privately and successfully write data to, and more than one database clients to privately learn about records from, an outsourced database.

Homomorphic encryption is every other privacy-keeping answer that is based totally on the idea of computing over encrypted facts without understanding the keys belonging to special events. To make certain confidentiality, the owner of the record can also encrypt data with a public key and store information inside the cloud. When the manner engine reads the facts, there may be no need to have the private key to decrypt the information. In private computation on encrypted genomic statistics, the authors proposed a privacy-keeping version for genomic statistics processing the usage of homomorphic encryption on genome-huge association studies[22].

Anonymization is some other approach to ensure the privacy of touchy records. Sail offers person-stage data on the availability of information types within a collection. Researchers are not capable of

Received: April 2, 2020 Revised: May 27, 2020 Accepted: June 25, 2020

DOI: 10.5281/zenodo.3909981

move-hyperlink (which is much like equality be part of in sq.) information from different out of doors research, because the identities of the samples are anonymized. In any other attempt [22] the authors advise an integration architecture to make it viable to perform aggregated queries over anonymized clinical facts units from specific information carriers. In this solution, statistics carriers take away the data topics' identifiers and practice -stage encryption the usage of hashing and PKI certificates. The touchy records will then be anonymized using an open-source toolkit and may be encrypted granularly the use of the cloud provider's public key.

6. Conclusions

This paper reviewed current advances in cloud computing security and privacy research. It defined numerous cloud computing key concepts and technology, including virtualization, and packing containers. The results which are presented within the location of cloud protection and privateness are based on cloud company. Protection and privacy factors that affect the activities of cloud carriers approximately the felony processioning of consumer records were diagnosed and a review of existing research was performed to summarize the trendy in the area.

References

[1] S. Pearson, "Privacy, security and trust in cloud computing," in Privacy and Security for Cloud Computing (S. Pearson and G. Yee, eds.), Computer Communications and Networks,

[2] E. U. Directive, "95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals about the Processing of Personal Data and the Free Movement of such Data," Official Journal of the EC, vol. 23, 1995.

[3] "Hypervisors, virtualization, and the cloud: Learn about hypervisors, system virtualization, and how it works in a cloud environment." Retrieved June 2015.

[4] M. Portnoy, Virtualization Essentials. 1st ed., 2012.Alameda, CA, USA: SYBEX Inc.

[5] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology (Special Publication 500-292). USA: CreateSpace Independent Publishing Platform, 2012.

[6] R. Pike, D. Presotto, K. Thompson, H. Trickey, and P. Winterbottom, "The use of namespaces in plan 9," SIGOPS Oper. Syst. Rev., vol. 27, pp. 72–76, Apr. 1993..

[7] M. A. Leandro, T. J. Nascimento, D. R. dos Santos, C. M. Westphall, and C. B. Westphall, "Multitenancy authorization system with federated identity for cloud-based environments using shibboleth," in Proceedings of the 11th International Conference on Networks, ICN 2012, pp. 88–93, 2012.

[8] G. Dreo, M. Golling, W. Hommel, and F. Tietze, "Iceman: An architecture for secure federated intercloud identity management," in Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on, pp. 1207–1210, May 2013.

[9] G. Sipos, D. Scardaci, D. Wallom, and Y. Chen, "The user support program and the training infrastructure of the EGI federated cloud," in High-Performance Computing Simulation (HPCS), 2015 International Conference on, pp. 9–18, July 2015.

[10] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, HotCloud'09, (Berkeley, CA, USA), USENIX Association, 2009.

[11] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh, "Terra: A virtual machine-based platform for trusted computing," in Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles, SOSP '03, (New York, NY, USA), pp. 193–206, ACM, 2003.

[12] S. Zhu and G. Gong, "Fuzzy authorization for cloud storage," Cloud Computing, IEEE Transactions on, vol. 2, pp. 422–435, Oct 2014.

[13] F. F. Brasser, M. Bucicoiu, and A.-R. Sadeghi, "Swap and play: Live updating hypervisors and its application to Xen," in Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security, CCSW '14, (New York, NY, USA), pp. 33–44, ACM, 2014.

Received: April 2, 2020 Revised: May 27, 2020 Accepted: June 25, 2020

DOI: 10.5281/zenodo.3909981

[14] C. Klein, A. Papadopoulos, M. Dellkrantz, J. Durango, M. Maggio, K.-E. Arnzen, F. HernandezRodriguez, and E. Elmroth, "Improving cloud service resilience using brownout-aware load balancing," in Reliable Distributed Systems (SRDS), 2014 IEEE 33rd International Symposium on, pp. 31–40, Oct 2014.

[15] E. Lakew, L. Xu, F. Hernandez-Rodriguez, E. Elmroth, and C. Pahl, "A synchronization mechanism for cloud accounting systems," in Cloud and Autonomic Computing (ICCAC), 2014 International Conference on, pp. 111–120, Sept 2014.

[16] Y. Huang and I. Goldberg, "Outsourced private information retrieval," in Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society, WPES '13, (New York, NY, USA), pp. 119–130, ACM, 2013.

[17] M. Gostev, J. Fernandez-Banet, J. Rung, J. Dietrich, I. Prokopenko, S. Ripatti, M. I. McCarthy, A. Brazma, and M. Krestyaninova, "SAIL - a software system for sample and phenotype availability across biobanks and cohorts," Bioinformatics, vol. 27, no. 4, pp. 589591, 2011.

[18] A. Gholami, E. Laure, P. Somogyi, O. Spjuth, S. Niazi, and J. Dowling, "Privacy-preservation for publishing sample availability data with personal identifiers," Journal of Medical and Bioengineering, vol. 4, pp. 117–125, April 2014.

[19] L. Zhou, V. Varadharajan, and M. Hitchens, "Integrating trust with cryptographic role-based access control for secure cloud data storage," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 560–569, July 2013.

[20] J. Sendor, Y. Lehmann, G. Serme, and A. Santana de Oliveira, "Platform level support for authorization in cloud services with OAuth 2," in Proceedings of the 2014 IEEE International Conference on Cloud Engineering, IC2E '14, (Washington, DC, USA), pp. 458–465, IEEE Computer Society, 2014.

[21] C. Klein, A. Papadopoulos, M. Dellkrantz, J. Durango, M. Maggio, K.-E. Arnzen, F. HernandezRodriguez, and E. Elmroth, "Improving cloud service resilience using brownout-aware load balancing," in Reliable Distributed Systems (SRDS), 2014 IEEE 33rd International Symposium on, pp. 31–40, Oct 2014.

[22] E. Lakew, L. Xu, F. Hernandez-Rodriguez, E. Elmroth, and C. Pahl, "A synchronization mechanism for cloud accounting systems," in Cloud and Autonomic Computing (ICCAC), 2014 International Conference on, pp. 111–120, Sept 2014.

Received: April 2, 2020 Revised: May 27, 2020 Accepted: June 25, 2020

DOI: 10.5281/zenodo.3909981