International Journal of Engineering & Technology, 7 (4.6) (2018) 241-245

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Recent Trends in Security and Privacy of Sensitive Data in Cloud Computing

Dayaker P[1]*, Chandrasekhara Reddy T[2], Honey Diana P[3], A. Mallikarjun Reddy[2]

[1]*Department of CSE, Holy Mary Institute of Technology and Science, Hyderabad, India*
[2]*Department of CSE, Anurag Group of Institutions, Hyderabad, India*
[3]*Malla Reddy College of Engineering and Technology, Hyderabad, India*
**Corresponding author E-mail: poreddydayakar2@gmail.com*

Abstract

Cloud Computing (CC) is reforming many biological communities by furnishing associations with registering assets including simple organization, network, design, Romanization, and adaptability. This change in perspective raises an expansive scope of security and protection issues that must be thought about. Multi-tenure, loss of control, and trust are entering challenges in cloud processing conditions. This paper surveys the current advancements and a wide show of both earlier and frontier extends on cloud security and protection. We classify the current look into as per the cloud reference engineering coordination, asset control, physical asset, and cloud benefit administration layers, in spite of inspecting the current improvements in security safeguarding touchy information approaches in CC, such as, security risk demonstrating and protection upgrading conventions and arrangements.

Keywords: *Use about five key words or phrases in alphabetical order, Separated by Semicolon.*

1. Introduction

CC is reforming a lot of our ecosystems, containing medical services. Thought about with earlier approaches for organizing data, CC circumstances offer typical benefits, such as, the availability of automated tools to collect, design plus reconfigure virtualized resources on request. These mark it very simple to attain organizational goals as relations can without much of a stretch send cloud supervisions. In some instance, move in the worldview that drives with the reception of CC is gradually contribution rise to security plus protection contemplations finding with types of CC, i.e., multi-occupancy, confide in, accountability [1]. Thus, cloud phases that handle tantalizing information are necessary to send specific procedures plus authoritative safeguards to avoid information security collapses that can result in enormous plus expensive damages.

Sensitive information with respects to CC incorporates data from a wide range of diverse regions plus controls. Data regarding health is a run of the typical case, of the kind of delicate data dealt with in CC conditions, and then obviously more people will want data recognized with their health to be secure. Subsequently, with the development of these novel cloud advancements lately, security plus information insurance prerequisites have advanced to secure persons against surveillance plus database expose. An insufficient cases of such protective enactment are the EU Data Protection Directive (DPD), [2] plus the US Health Insurance Portability, plus Accountability Act (HIPAA) [3], both of which request security preservation for enchanting care of actually recognizable data.

This paper exhibits a review of the exploration of security and protection of delicate information in a cloud registering conditions. We recognize new advancements in the territories of an organization, asset control, physical equipment, plus cloud benefit administration stages of a cloud provider. We to survey the best in class insecurity saving delicate information approaches for dealing with touchy information in CC, for instance, security risk displaying plus protection progressing conventions plus arrangements.

2. Key Concepts and Technologies

In the development of current years, significant IT merchants, like Amazon, Microsoft, plus Google have set virtual machines (VM), through their clouds that clients could hire. These clouds use equipment resources plus bolster live relocation of VM addition to powerful load-adjusting plus on request provisioning. This indicates, by hiring VM through a cloud, the complete server farms the impress of an advanced project can be reduced from a vast number of physical servers to a pair hundreds of hosts.

While it is useful plus cost effective to consume CC thusly, there can be problems with security when operating frameworks that are not given in-house. To examine these plus discover suitable measures, there are a few key thoughts plus advances that are normally used as a part of CC that should be seen, i.e. virtualization systems, assortments of cloud administrations, plus "holder" innovations.

2.1. Virtualization Mechanisms

A hypervisor is a significant part that dwells between VM also, equipment to regulate the virtualized resource [4]. It gives the mode to run a few confined virtual machines on the similar physical host. Hypervisors can be organised into two gatherings [5]:

- Category I: Here the hypervisor runs straightforwardly on the genuine framework equipment, plus there is nope operating system (OS) under it. This method is proficient as it wipes out some middle person layers. Additional advantage with this kind of hypervisor is that security stages can be enhanced by segregating the visitor VM. That way, if a VM is traded off, it may just influence itself plus won't meddle with the hypervisor or another visitor VM.

- Category II: This kind of hypervisor keeps running on a facilitated OS that gives virtualization administrations, for example, input/output (IO) gadget support plus memory administration. All VM cooperation's, for example, IO asks for, arrange activities and interferes, are taken care of by the hypervisor. Xen and kernel virtual machine (KVM) are well-known open-source hypervisors. Xen runs openly on the fundamental equipment and it embeds a virtualization layer among the framework equipment plus the VM. The OS running in the VM co-operate with the virtual assets, as though they were really physical assets. KVM is a virtualization included in the Linux Kernel that marks it conceivable to securely execute visitor code specifically, on the host CPU.

2.2. Characteristics

While considering CC, we must know about the types of administrations that are advertised, the way those administrations are carried to those consuming the administrations, plus the distinctive categories of individuals what's more, bunches that are involved with cloud administrations.

CC delivers registering programming, stages, plus foundations as administrations in view of pay-as-usage models. Cloud benefit models can be conveyed for on-request stockpiling plus figuring authority in different courses: Software as a Service (SaaS), Platform as a Service (PaaS) furthermore, Infrastructure as a Service (IaaS). CC administration models have been developed amid a previous couple of years inside an assortment of regions utilizing the "as-a-Service" idea of cloud registering, for example, Business Integration as a Service, Cloud-Based Analytics as a Service (CLAaaS), Data as a-Service (DaaS). This paper states to the NIST cloud benefit models highlights [6] that are outlined in Table 1 that may be conveyed to shoppers utilizing diverse models, i.e., a private cloud, group cloud, open cloud.

The NIST CC reference design [7], characterizes five main performers in the cloud field they are first one is cloud consumers, second one is providers, third one is carrier, next one is auditors plus last one is brokers. Every of these on-screen characters are an element (either a man or an association) that takes an interest in a cloud registering exchange or process, as well as achieves CC errands. A cloud consumer is an association that utilizations administrations from cloud suppliers in the setting of a business association. A cloud provider is a substance marks cloud facilities accessible to intrigued clients. A cloud auditor conducts autonomous evaluations of cloud facilities, tasks, execution plus security in connection to the cloud deployment. A cloud broker is a, substance that deals with the utilization, execution, plus conveyance of cloud services, plus furthermore builds up connections among cloud providers plus cloud consumers. A cloud carrier is an element that gives network plus transport of cloud facilities from cloud suppliers to cloud buyers through the physical organisations [8].

Table 1: Classification of Cloud Service Models plus Features

Server Model	Function	Example
SaaS	Enables customers to run uses by virtualizing equipment on the assets of the cloud suppliers	Sales force Customer Relationship Management
PaaS	Gives capacity of conveying custom uses with their conditions inside condition called a holder.	Google App Engine4, Heroku
IaaS	Gives an equipment stage as an administration such as virtual machines, handling, stockpiling, systems plus database administrations	Amazon Elastic Compute Cloud

The exercises of cloud suppliers can be classified into five principles: service deployment, resource abstraction, physical resources, service management, security plus privacy [7]. The security plus protection comprises that are vital for the exercises of cloud providers are depicted in Table 2 [10].

Table 2: Security plus Privacy Features of the Cloud Suppliers

Security Context	Description
Authentication plus Authorization	Authentication plus authorization of cloud users using pre-defined Identification systems.
Identity plus Access Management	Cloud user provisioning plus provisioning via heterogeneous cloud service suppliers.
Confidentiality, Integrity, Availability	Assuring the confidentiality of the information objects, authorizing information modifications plus ensuring that services are offered when required.
Monitoring plus Incident Response	Continuous observing of the cloud infrastructure to promise compliance with user security policies plus auditing Requirements.
Policy Management	Defining and enforcing rules for certain actions like auditing.
Privacy	Protect personally recognizable data (PII) within the cloud from adversarial attacks that aim to discover out the identity of the individual that PII relates to.

The dominant part of CC foundations comprises of dependable administrations conveyed through server farms to accomplish high accessibility through repetition. A server farm or PC focus is an office used to house PC frameworks and related segments, units [9].

3. Security and Privacy Challenges in Cloud

CC has raised some security risks, i.e., information ruptures, information misfortune, refusal of the benefit, and pernicious insiders that have been broadly examined. These dangers for the most part begin with issues, i.e., multi-tenure plus trust [11].

3.1. Security Issues in CC

• ***Multi-tenure:*** Multi-occupancy refers to sharing physical gadgets plus virtualized assets between different independent clients [12]. Using this sort of course of act infers that an assailant could be on an indistinguishable physical machine from the unbiased. Cloud providers utilize multi-occupancy highlights to assemble, frameworks that can effectively scale to meet clients' needs; nonetheless, the sharing of resources infers that it can be less demanding for an assailant to access the object's information.

• ***Loss of Control:*** Loss of control is potential rupture of security that can happen where shoppers' information and assets are facilitated at the cloud supplier's claimed locations. As the clients don't

have unequivocal control over their information, this marks it workable for cloud suppliers to make information mining over the clients' information, which can lead to security issues. Furthermore, when the cloud supplier's strengthening information at the various information focuses, the customers can't make certain that their information is completely deleted all around when they erase their information. This can possibly prompt abuse of the unerased information. In these types of conditions where the shoppers lose control over their information, they see the cloud supplier as a black-box where they can't openly screen the assets openly [12].

• ***Trust Chain in Clouds*:** Trust adopts a vigorous part of drawing in most customers by assuring on cloud providers [29]. As of loss of control, cloud clients rely on the cloud providers using put stock in components as a contrasting choice to providing clients upfront control over their information plus cloud assets. Hence cloud providers assemble certainty among their clients by ensuring them that the supplier's tasks are affirmed inconsistency with confident shields plus principles.

3.2. Privacy Sensitive Data Processing

The security problems in CC, lead to various protection concerns. Security is the complex point that has distinctive interpretations relying upon settings, societies, and groups [13]. A few exertions have been made to hypothesise protection by investigators, keeping in mind the end goal to give us a superior comprehension of protection – for the case, Alan Westin's examination is thought to be the main noteworthy, work on the problem of buyer information security plus information insurance. Westin [14] characterized security as taking after.

"Security is the claim of people, gatherings, or foundations to decide for themselves whenever, how, and to what degree data about them is imparted to others [33]. " The new directions consider forcing huge punishments for protection ruptures that outcome from infringement of the directions, for instance, such a punishment could be 0.5 percent of the around the world yearly throughput of the culpable venture

4. Security Solutions

This segment surveys the examination on security arrangement, for example, verification, approval, and personality administration that existed in Table 2 [10] as presence important so that the exercises of cloud suppliers are adequately safe.

4.1. Authentication plus Authorization

Executions of cloud security arrangements under the idea of Security as a Service are in their getting up stage. This exploration has proposed a cloud security framework in view of that idea and made commitments in the territory of confirmation and approval administrations for a cloud domain. The issue has been illuminated and the goals have been accomplished [17].

The implementations of the proposed cloud security framework comprise of two segments: focal security servers and entrance security servers. Focal security servers are capable to give two-character administrations, for example, validation and approval administrations for cloud-based programming administrations. Both character administrations were planned utilizing Web Service innovation and XML-based measures. Entryway security servers are dependable to ensure cloud entryways in view of the administrations conveyed from focal security servers. Entryway security server plays the part of an intermediary server, which gives Policy Implementation Point administrations to application administrations of a cloud gateway [19]. Along these lines, confirmation and approval arrangements are decoupled from singular application administrations and appointed to the mutual cloud security framework, which convey these character benefits through SaaS show. Centralization and sharing of those character benefits in a different security framework brings about a successful and adaptable answer for a cloud domain [20]. This approach empowers the whole cloud security framework to be controlled and overseen considerably less demanding, subsequently raising the nature of gave cloud security arrangements. Moreover, the framework guarantees the provisioning of those personality benefits in a safe and solid way [21].

A model of approval benefit has been executed so as to exhibit the conceivable utilization of the planned cloud approval framework. It is a part based approval framework with negligible fundamental highlights. This model usage comprises of two sections: approval administration and access control organization. The approval benefit is actualized utilizing Web Service innovation and access control organization is actualized with improved usefulness as an easy to understand electronic application. Through this exploration an answer accommodated fabricating cloud-based character administrations, for example, confirmation and approval in view of the cloud SaaS show. This arrangement means to give an open and stage autonomous engineering of a cloud security framework, which is totally benefit situated, in this way empowering the framework to be versatile, interoperable, approximately coupled and area straightforward.

4.2. Identity and Access Management

The Cloud Security Alliance (CSA) distinguishes the accompanying major IAM capacities basic for fruitful and powerful administration of characters in the cloud [34]:

- Identity Provisioning/de-provisioning – secure and auspicious administration of on-boarding and off-boarding clients in the cloud
- Authentication – incorporates contemplations for validation related difficulties, such as, certification supervision plus assigned verification.
- Federation – secure trade of character properties between the specialist co-op (SP) and Identity Provider (IdP) and answers for deliver challenges as for character life cycle administration, accessible confirmation techniques to secure classification, and trustworthiness while supporting non-renouncement.
- Authorization and client profile administration – incorporates setting up trustworthy consumer profile plus arrangement information, using it to control get to intimate the cloud assistance plus doing this in an audible mode. The outline should cause in the above and guarantee that consistence is a key thought all through.

Client and gathering strategies should be characterized at this stage [28]. Watchful thought should be given to strategy arrangement and should be done in dialogs with partners to keep ideal harmony between security what's more, simple entry.

4.3. Confidentiality, Integrity, and Availability

Confidentiality

Privacy is commonly comparable to protection. Procedures tried to assurance privacy intended to retain touchy information from communicating the erroneous persons, while confirming that the ideal persons can in certainty get it [17]. Again, defending data organization can contain extraordinary formulating for those conscious of such archives. Such formulating would ordinarily join security risks that could undermine this information. Preparing can help acquaint appropriate people with chants issues plus how to make preparations for them. Encourage portions of preparing may incorporate solid secret code plus watchword related set of rules [27].

Integrity

Integrity embraces keeping up the uniformity, correctness, plus dependability of data over its total life cycle. Information should not be altered in travel, plus steps should be taken to guarantee that information can't be adjusted by unauthorised individuals [26]. These procedures integrate record consents and clients get to controls. Variant control possibly used to avoid, mistaken changes or unintentional erasure by approved clients turning into an issue. What's more, a few means must be set up to recognize any modifications in data that can happen because of non-human-caused occasions, i.e., an electromagnetic heartbeat (EMP) or server crash.

Availability

Availability is finest assured by systematically keeping up all equipment, performing equipment repairs promptly when mandatory plus keeping up an efficiently working framework form that is free of programming clashes. It's likewise important to retain recent with all vital framework redesigns. Giving acceptable correspondence transmission capacity plus possession the event of bottlenecks is equally imperative. Protections against data misfortune in associations essential incorporate erratic occasions, i.e., cataclysmic events plus fire. To keep data misfortune from such events, a reinforcement duplicate might be put away in a topographically separated area, maybe even in a flame resistant, waterproof safe [25].

4.4. Security Policy Management

As new applications are included or the availability necessities for existing ones are adjusted arrange activities and security overseers must have the capacity to survey the basic firewall rules and changes that are required, and start the right change administration work process for execution. Be that as it may, application availability prerequisites are once in a while reported, not to mention kept up, with many associations depending on spreadsheets, sometimes refreshed databases, and colleagues' recollections for this data. This rolls out significant exchanges about required improvements with application proprietors also; others - who don't normally talk in the dialect of ports and conventions - close unthinkable [32].
Embracing an application-driven way to deal with security strategy administration will allow associations to beat these difficulties. Application-driven examination that is completely coordinated in a security administration arrangement can computerize the change work process and address basic difficulties, such as [15],

- Identifying the effect of proposed arrange changes, such as, server relocations or new steering what's more, division plans, to the association's applications.
- Accurately distinguishing/evacuating access rules for decommissioned applications, without affecting the availability of different applications.
- Determining the effect of proposed changes to get to rules — for instance, because of newfound dangers or vulnerabilities — to an association's applications.
- Using application network prerequisites as a layer of reflection to help veil the developing multifaceted nature of the present security strategies.
- Bridging the correspondence holes between the distinctive voting public inside IT. [24]

5. Privacy for Sensitive Data

Over the period, associations have gathered vital information concerning the individuals in our social orders that contain touchy data [30]. Specialists got to get to and dissect such data utilizing large data advancements in CC, whereas associations are needed to uphold data insurance consistence.

There has been a major advance on security conservation for touchy data in each trade moreover, the bookish community, e.g., arrangements that make conventions and apparatuses for cryptography of data for privacy functions. This section orders business concerning this territory as per various security insurance requirements [16]. In any case, these arrangements haven't however been loosely received by cloud specialist organizations or associations.

Pearson [1] examines a scope of security and protection challenges that a raised by CC. The absence of shopper management, the absence of getting ready and talent, unapproved auxiliary utilization, the unpredictability of body consistency, trans border data stream confinements and case are among the difficulties looked in CC things within the creators depict the protection difficulties of genomic data within the cloud together with terms of administrations of cloud suppliers that don't seem to be created with a medicative services outlook, familiarity with the patient to transfer their data into the cloud while not their assent, multi-tenure, data checking, data security, and responsibility. The creators likewise provide suggestions to data proprietors once expecting to utilize cloud provider administrations [23].

In the creators talked a couple of few protection problems concerning genomic sequencing [35]. This the examination likewise pictured many open analysis problems, (for example, outsourcing to cloud suppliers, genomic data cryptography, replication, honesty, and evacuation of genomic information) aboard giving recommendations to reinforce security through a coordinated effort between varied parts and associations. In another travail, crude genomic data reposting through encoded short peruses is projected [21].

Outsourcing guard is extra theme that's examined. The creators describe the concept of "outsourcing protection" wherever an information man of affairs refreshes the information once your time on untrusted servers [22]. This definition accepts that information customers plus also the untrusted servers don't seem to be able to get the suspend of something concerning the substance of the databases while not approved access. The Creators execute a server-side ordering structure to deliver a framework that allows a solitary information man of affairs to on the QT and proficiently compose data to, and diverse information customers to on the QT scan data from, outsourced information.

In the define and execution of a security structure for Bio bank Cloud, a phase those backings the safe reposition and getting ready of genomic data within the CC conditions are talked concerning [31]. The projected system is predicated on the cloud protection danger displaying approach that is employed to characterize the protection risk demonstrate for handling last sequencing data as per the DPD [2]. This procedure includes AN filmable dual-factor authorization plus an RBAC get to control system, withal examining instruments, to ensure that the conditions of the DPD are glad [18].

6. Conclusion

This paper overviewed late improvements in CC security plus protection look into. It depicted a few CC significant ideas plus innovations, for example, virtualization, plus holders. We likewise talked about some security challenges that are elevated by existing or imminent security enactment, for example, the EU DPD plus the HIPAA. The outcomes that are displayed in the zone of cloud

security plus protection depend on cloud supplier exercises, for example, giving the organization, asset deliberation; physical asset and cloud benefit administration layers. Security plus protection aspects that impact the exercises of cloud providers in association to the lawful processioning of client data were recognized plus an audit of existing exploration was led to summarize the best in class in the field.

References

[1] S. Pearson, "Privacy, security and trust in CC ," in Privacy and Security for CC (S. Pearson and G. Yee, eds.), Computer Communications and Networks, pp. 3–42, Springer London, 2013.

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

[3] U. States., "Health insurance portability and accountability act of 1996 [micro form] : conference report (to accompany h.r. 3103)." http://nla.gov.au/nla.catvn4117366, 1996.

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

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

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

[7] R. Dua, A. Raja, and D. Kakadia, "Virtualization vs containerization to support paas," in Cloud Engineering (IC2E), 2014 IEEE International Conference on, pp. 610–614, March 2014.

[8] D. Bernstein, "Containers and Cloud: From LXC to Docker to Kubernetes," IEEE CC , vol. 1, no. 3, pp. 81-84, 2014.

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

[10] NIST Special Publication 500–291 version 2, NIST CCStandards Roadmap, July 2013, Available at http://www.nist.gov/itl/cloud/publications.cfm.

[11] B. Russell, "Realizing Linux Containers (LXC)." http://www.slideshare.net/BodenRussell/linuxcontainers next-gen-virtualization-for-cloud-atl-summit-ar4-3-copy. Retrieved October 2015.

[12] U. S. F. Law, "Right to financial https://epic.org/privacy/rfpa/, 1978. privacy act of 1978."

[13] United Nations, "The Universal Declaration of Human Rights."http://www.un.org/en/documents/udhr/index.shtml, 1948. Retrieved August 2015.

[14] A. Westin, Privacy and Freedom. New Jork Atheneum, 1967.

[15] D. Bigo, G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz, and A. Scherrer, "Fighting cyber crime and protecting privacy in the cloud." European Parliament, Policy Department C: Citizens' Rights and Constitutional Affairs, October 2012.

[16] S. Stalla-Bourdillon, "Liability exemptions wanted! internet intermediaries' liability under uk law," Journal of International Commercial Law and Technology, vol. 7, no. 4, 2012.

[17] N. Mimura Gonzalez, M. Torrez Rojas, M. Maciel da Silva, F. Redigolo, T. Melo de Brito Carvalho, C. Miers, M. Naslund, and A. Ahmed, "A framework for authentication and authorization credentials in CC ," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 509–516, July 2013.

[18] R. Banyal, P. Jain, and V. Jain, "Multi-factor authentication framework for CC ," in Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on, pp. 105–110, Sept 2013.

[19] R. Lomotey and R. Deters, "Saas authentication middleware for mobile consumers of iaas cloud," in Services (SERVICES), 2013 IEEE Ninth World Congress on, pp. 448–455, June 2013.

[20] H. Kim and S. Timm, "X.509 authentication and authorization in fermi cloud," in Utility and CC(UCC), 2014 IEEE/ACM 7th International Conference on, pp. 732–737, Dec 2014.

[21] B. Tang, R. Sandhu, and Q. Li, "Multi-tenancy authorization models for collaborative cloud services," in Collaboration Technologies and Systems (CTS), 2013 International Conference on, pp. 132–138, May 2013.

[22] 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.

[23] 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. infrastructure of the egi federated cloud," in High Performance Computing Simulation (HPCS), 2015

[24] C. Klein, A. Papadopoulos, M. Dellkrantz, J. Durango, M. Maggio, K.-E. Arzen, F. Hernandez- Rodriguez, and E. Elmroth, "Improving cloud service re silience using brownout-aware loadbalancing," in Reliable Cloud Systems (SRDS), 2014 IEEE 33rd International Symposium on, pp. 31–40, Oct 2014.

[25] 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.

[26] M. Anand, "Cloud monitor: Monitoring applications in cloud," in CCin Emerging Markets (CCEM), 2012 IEEE International Conference on, pp. 1–4, Oct 2012.

[27] A. Brinkmann, C. Fiehe, A. Litvina, I. Lück, L. Nagel, K. Narayanan, F. Ostermair, and W. Thronicke, "Scalable monitoring system for clouds," in Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and CC , UCC '13, (Washington, DC, USA), pp. 351–356, IEEE Computer Society, 2013.

[28] J. Nikolai and Y. Wang, "Hypervisor-based cloud intrusion detection system," in Computing,Networking and Communications (ICNC), 2014 International Conference on, pp. 989–993, Feb 2014.

[29] C. Basescu, A. Carpen-Amarie, C. Leordeanu, A. Costan, and G. Antoniu, "Managing data access onclouds: A generic framework for enforcing security policies," in Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on, pp. 459–466, March 2011.

[30] H. Takabi and J. Joshi, "Policy management as a service: An approach to manage policy heterogeneity in CCenvironment," in System Science (HICSS), 2012 45th Hawaii International Conference on, pp. 5500–5508, Jan 2012.

[31] K. W. Hamlen, L. Kagal, and M. Kantarcioglu, "Policy enforcement framework for cloud data management.," IEEE Data Eng. Bull., vol. 35, no. 4, pp. 39–45, 2012.

[32] S. Fischer-Hubner, J. Angulo, and T. Pulls, "How can cloud users be supported in deciding on, tracking and controlling how their data are used" in Privacy and Identity Management for Emerging Services and Technologies (M. Hansen, J.-H. Hoepman, R. Leenes, and D. Whitehouse, eds.), vol. 421 of IFIP Advances in Information and Communication Technology, pp. 77–92, Springer Berlin Heidelberg, 2014.

[33] E. Ayday, J. Raisaro, U. Hengartner, A. Molyneaux, and J.-P. Hubaux, "Privacy-preserving processing of raw genomic data," in Data Privacy Management and Autonomous Spontaneous Security (J. Garcia-Alfaro, G. Lioudakis, N. Cuppens-Boulahia, S. Foley, and W. M. Fitzgerald, eds.), vol. 8247 of Lecture Notes in Computer Science, pp. 133147, Springer Berlin Heidelberg, 2014.

[34] 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.

[35] K. Lauter, A. Lopez-Alt, and M. Naehrig, "Private computation on encrypted genomic data," Tech. Rep. MSR-TR-2014-93, June 2014.