I.J. Information Technology and Computer Science, **2022, 3, 52-61**
Published Online June 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2022.03.05

Ontologies as Building Blocks of Cloud Security

Naila Samad Shaikh[1], Affan Yasin[2], Rubia Fatima[2]
[1]Bahauddin Zakariya University Multan Pakistan
[2]Tsinghua University, Beijing, China
E-mail: nailasheikh1@gmail.com, affan.yasin@outlook.com, rubiafatima91@hotmail.com

Received: 02 October 2021; Accepted: 11 March 2022; Published: 08 June 2022

Abstract: Much like other processing domains, cloud computing is not surely safe. Security of cloud processing needs the same attention as any other aspect of cloud processing requires. Cyber world is shifting toward ontological technique and web 3.0 or web semantics for security. Cloud hosts servers demand more attention in context of security as number of resources and their access increases. Security measures have to be more extensive in cloud. Semantic web is usually new revolution inside the web science, which usually works upon base of ontologies. Ontologies are receiving great attention in the domain of computing and hence in the domain of security. This review paper examines different proposed "ontology centered techniques" and also provides a comprehensive analysis on these tactics. This research paper gives critical analysis of different models presented by different authors and researchers for ensuring security of a cloud based environment. This analysis helps different vendors of cloud technology to adapt one or all of these models to practically implement in their cloud machines whether they are offering IaaS, PaaS or SaaS. Any new security model using ontologies can also be proposed based on this study, as this paper gives a comprehensive comparison of the previously proposed ontologies for monitoring security state of cloud environment as safe or malicious.

Index Terms: Cloud Computing, Web Semantics, Ontologies, Cloud Security, Cyber Security, Information Security.

1. Introduction

Cloud computing can be a new area in processing environment which usually emphasize upon providing just about every computing facility required by end users on cloud, rather than providing each service on user machine. Much like other processing domains, cloud computing is not surely safe. Apart coming from development mindset, security part of cloud processing needs the same attention as any other aspect of cloud processing requires.

As well as traditional information security actions, new processing world is shifting toward ontological technique for security, as the entire computing world is shifting toward web 3. 0 or perhaps web semantics. Ontologies undoubtedly are a revolution in computing or perhaps programming area, so it can be equally productive in building security ontologies.

Major variation between traditional computing environment along with a cloud processing environment will be that cloud is partitioned in to multiple unbiased "virtual" hosts, all operating independently in addition to appearing towards the user to become a single real device. Such exclusive servers will be in essence disassociated from other physical server, with this extra flexibility, they are often moved about and scaled way up or down about the fly without affecting the final user. Such exclusive hosts demand more attention in context of security as number of resources and their access increases. Security measures have to be more extensive in cloud. Semantic web is usually new revolution inside the web science, which usually works upon base of ontologies. Ontologies are receiving great attention in the domain of computing and hence in the domain of security.

Cloud computing is practice of providing "computing" services to its users, either human users or machines, via a remote server located somewhere unknown to user (hence termed as the term "cloud server").

According to definition of cloud computing by National Institute of Standards and Technology NIST [9] "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing provides cloud services from remotely located cloud servers connected via network, i.e. internet. As it is an open secret that internet is pretty unsafe place in terms of information security, so the question has raised about the security of data hosted on cloud servers.

Traditional approaches to ensure information security proved insufficient in context of cloud computing. One has to find some totally different approach for security of cloud.

World is leading towards web 3.0 or semantic web. Ontologies are getting well deserved worth among the different technologies. Ontologies can be used effectively in proposing models for ensuring the security of all architectures of cloud computing either IaaS, PaaS or SaaS.

Different researchers proposed different models of ontologies for ensuring the security of said field. In this paper we are going to present a comprehensive analysis of these proposed models.

After analyzing all these models, one would be able to propose a new model, keeping in mind strengths and weaknesses of all previously proposed models.

An efficient cloud computing model has been described in [17].

2. Security of Cloud Computing

There is a lot to discuss about cloud computing environment. Security is a major concern amongst both existing and potential customers of cloud [7].

Regardless of which vendor provides cloud services, some standards are developed and followed by international monitoring authorities like Information Technology Infrastructure Library –ITIL and ISO/IEC 27001/27002 [15] [16] for security of cloud.

In 2009, International Data Corporation (IDC) conducted a survey [14] of 263 IT executives as cloud users to represent their opinions and understand their companies' use of IT cloud services. Security ranked first as the greatest challenge or issue of cloud computing.

According to careful early investigations on security level of cloud computing conducted by the Application Defense Center, assess that at least 92% of Web applications are vulnerable to some form of attack [12].

Another survey found that about 75% of all attacks against web servers, target web based applications [13]

Ensuring security for cloud computing is such an important parameter that there are a large number of documents approved by different federal governments and regulatory authorities which emphasize on rules and regulations for enforcing security on cloud.

Such an important document is "Procure Secure - A guide to monitoring of security service levels in cloud contracts" [8], published by ENISA in spring 2012.

Similarly, "The Cloud Security Alliance Cloud Controls Matrix" (CCM) [11] is a security control framework especially designed to help Cloud customers assess the security risk of a Cloud provider.

In the same way, another guideline is "The FedRAMP Security Controls Baseline" [10] which includes a set of security controls that Cloud service providers must apply in order to fulfil FedRAMP requirements.

A comprehensive work to detect intrusion has been discussed in [18] as well.

In this review, we will discuss only the issue of security of cloud computing. Different researchers presented different views about it.

Different mechanisms are there in commercial use for making cloud secure. One of the mechanisms is the security via web semantics i.e., semantics web languages and technologies are being used to enhance security of cloud environments. Different ontologies are proposed by different authors and researchers. We will analyze a few of these ontologies.

3. Main Issues of Cloud Security

There are a lot of aspects to discuss, in regards of security of cloud computing environment. A few issues are shown in the fig 1 below. Top issues in cloud computing are as follows, shown in fig.1. These issues are highlighted in [4,5]

- Privacy and security

The privacy of cloud itself and the data hosted on cloud doesn't ensure its privacy and security.

- Context Awarenesses

Cloud service provider is not aware of context uploaded and it may or may not be illegal and prohibited material.

- Data Management

Data Management is a tedious task in sense of resource allocation.

- Servive level operational issues

At the end of cloud service provider, there are a lot of operational level issues which needs to be cattered very carefully.

- End user

Authenticity of end user is also another major issue in case of cloud computing environment.

- General Cloud Security

Prevention from unauthorized access is a major concern in cloud environment in general and also main topic of concern in this study as well.

- Mobile Cloud Security

Major aim behind the idea of cloud computing is that data should be accessible to anyone, anywhere and any device on the go. But this concept itself is a concern of security in terms of authorized or unauthorized access.

- Privacy

Is data accessible to someone else outside the cloud or the service provider may be a concern for the end user.

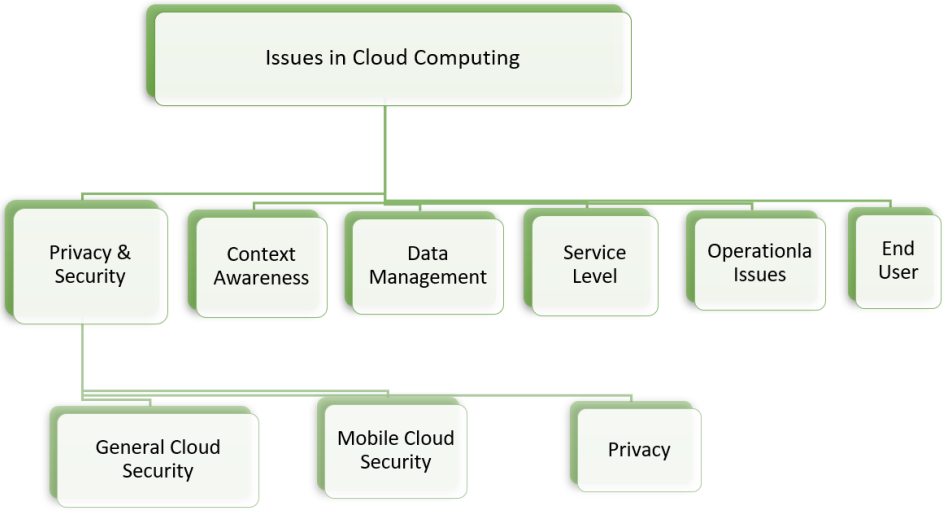


Fig.1. Issues in Cloud Computing

This figure discusses all the general issues in cloud environment. In this review paper, we will focus only on the issues related to security and privacy of cloud computing environment.

4. Major Pillars of Security

Major pillars of security of cloud computing environment which should be addressed while developing a system to ensure security of a cloud, as discussed by [5] are following.

- Confidentiality
- Integrity
- Authenticity
- Availability
- Privacy
- Trust
- Audit and compliance

All these issues of security need to be properly addressed in cloud especially, because the major concern in cloud computing is that processing goes in hands of third party, not in the control of user or providers of cloud, so care should be taken in providing all these security issues.

A few issues and challenges in security of cloud computing has been discussed by K. Popović, Ž. Hocenski and H. Tianfieldin [4,5]. Their distribution of responsibilities among cloud service provider and cloud user is depicted in Table1.

Table 1. Security Issues in cloud computing

Model	Responsibility of	Cloud Provider	Service Provider	Cloud Customer
IaaS	VM's Security			Responsible
	Secured VM image Repository	Responsible		
	Securing VM boundaries	Responsible		
	Hypervisor Security	Shared Responsibility	Shared Responsibility	
PaaS	SOA (Service Oriented Architecture) related Security	Shared Responsibility		Shared Responsibility
	API Security		Responsible	
SaaS	SaaS Security	Shared Responsibility	Shared Responsibility	
	Web Application Security	Responsible		

Cloud Security concerns

Cloud security can be categorized in three different aspects [5]

- ***Identity security:*** end-to-end security, especially authentication of user and cloud providers as well.
- ***Information security:*** control on physical access and third-party control
- ***Infrastructure security***: whole infrastructure of cloud should be made secure including switches, routers, network, devices and data

5. Different Proposed Ontologies for Cloud Security

An ontology to perceive the current security state of network has been proposed by [1] in their paper *"Ontology Based Approach for Perception of Network Security State."*

According to Hansman [6] a high-quality ontology should have following characteristics

- Completeness
- Mutually exclusive
- Unambiguous
- Acceptable
- Determinism
- Comprehensible
- Repeatable
- Constant and defined Terminology
- Useful

But [6] also stated that an ontology cannot always fulfill all the requirements.

The ontology by [1] in tool Protégé is shown in the figure2 below. Their ontology contains classes Actor, Attack, Network and Vulnerabilities.

Subclasses of these classes are following

Network class contains subclasses as

- Hardware components
- NOS
- Roles
- Users
- Services

Actor class has subclasses as

- Attack Goal
- Scope
- Automation Level
- Actor Location
- Effect

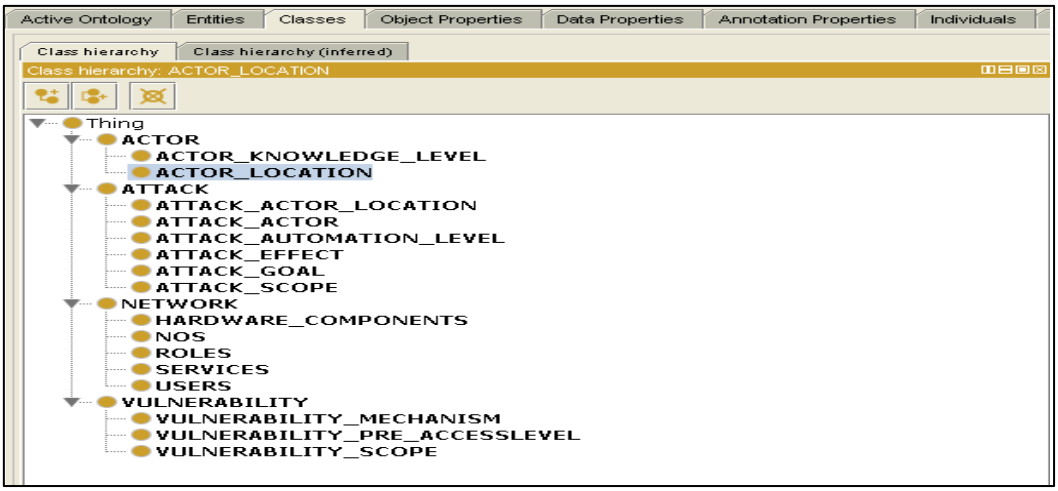


Fig.2. Class hierarchy of the proposed ontology

According to [3], the purpose of ontology is

- To share common understanding of the structure of information among people or software agents
- To permit reuse of domain knowledge
- To make domain assumption explicit
- To separate domain knowledge from the operational knowledge
- To analyze domain knowledge

In this context, their ontology is given in the figure 3 below.

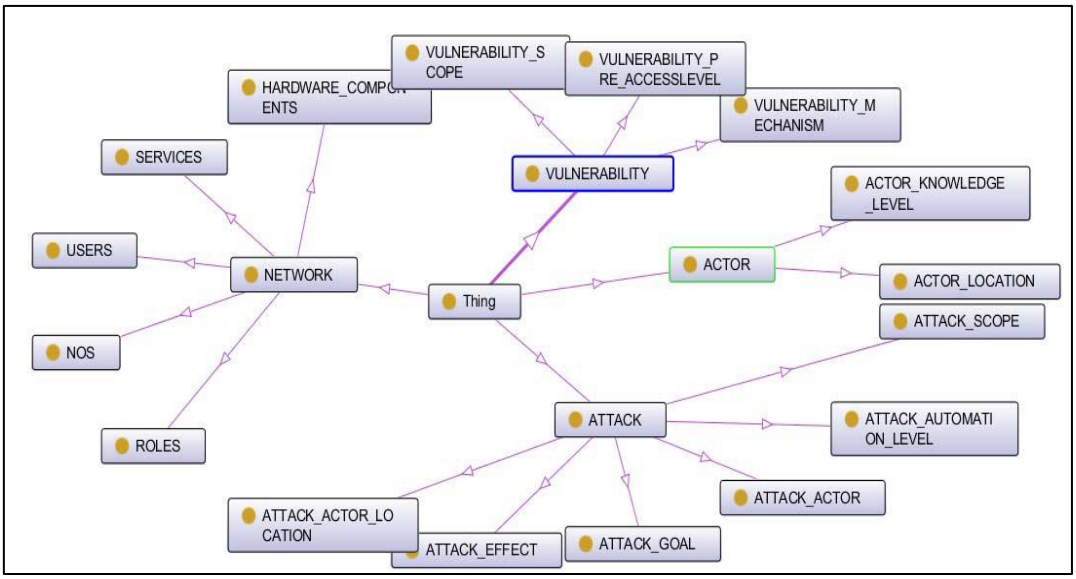


Fig.3. Class visualization of proposed ontology

Their prediction rules are as follows, shown in flow chart in figure 4.

If (actor_location is foreign)
AND (automation level is automatic)
AND (Goal is to destroy data)
AND (scope is large network)
AND (effected service is more than threshold value) then state is ***unsafe.***

Or If (actor_location is local)
AND (automation level is manual)
AND (Goal is to read data)

AND (scope is small private network)
AND (effected service is less than threshold value) then state is moderately ***safe.***

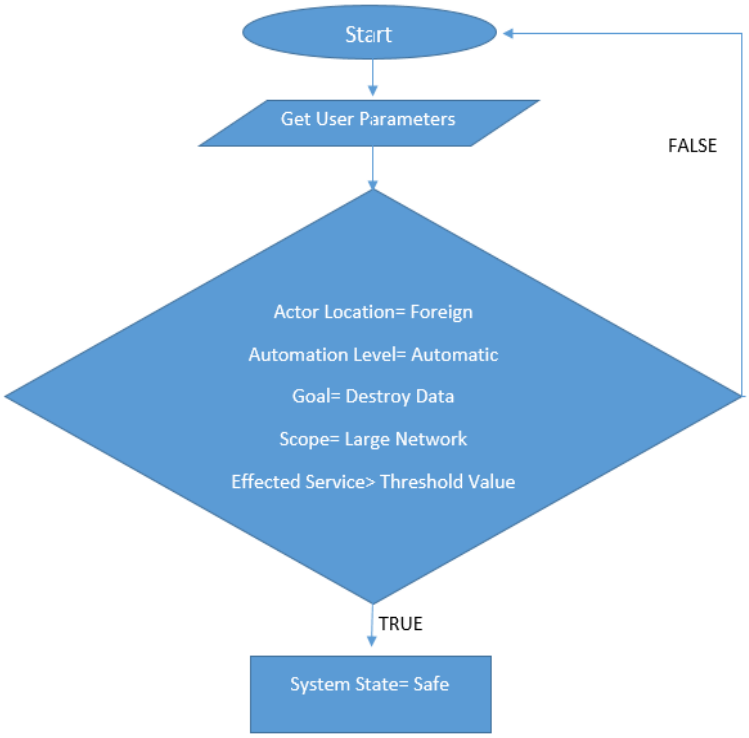


Fig.4. Flow Chart of proposed ontology

This ontology is very simple and straightforward, however this ontology is unable to detect unauthorized access attacks, so adding the classes of role base access control could extend this ontology. Moreover, ontology can also be extended to detect normal and malware attack parameters like turnaround time of services, response time and through put etc. Another ontology is proposed [2] by Karin Bernsmed, Astrid Undheim, Per H˚akon Meland and Martin Gilje Jaatun in their paper *"Towards an Ontology for Cloud Security Obligations"*. The paper proposes another ontology for security of cloud which has two main classes, i.e., *"Cloud Services"* and *"Cloud security obligations"* this ontology somehow tries to fulfil the flaws of previously discussed [1] ontology but it is still incomplete itself. Cloud service class presents *SaaS, IaaS and PaaS* services as shown in the figure 5 below.

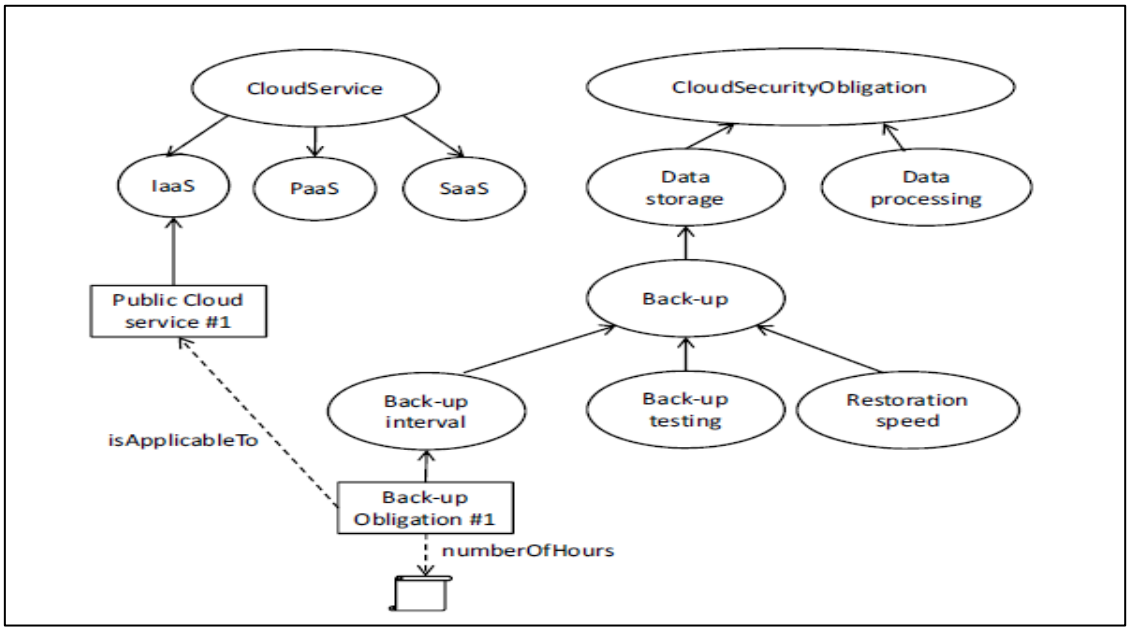


Fig.5. Cloud security obligations ontology: sample concepts

The second class in this ontology is CLOUD SECURITY OBLIGATIONS, which is discussed in more detail. This class has following subclasses: Data Storage, Data Transfer, Data Processing, Access Control, Security Procedures, Incident Management, Privacy and Hybrid Clouds. The ontology in tool protégé is shown in figure 6.

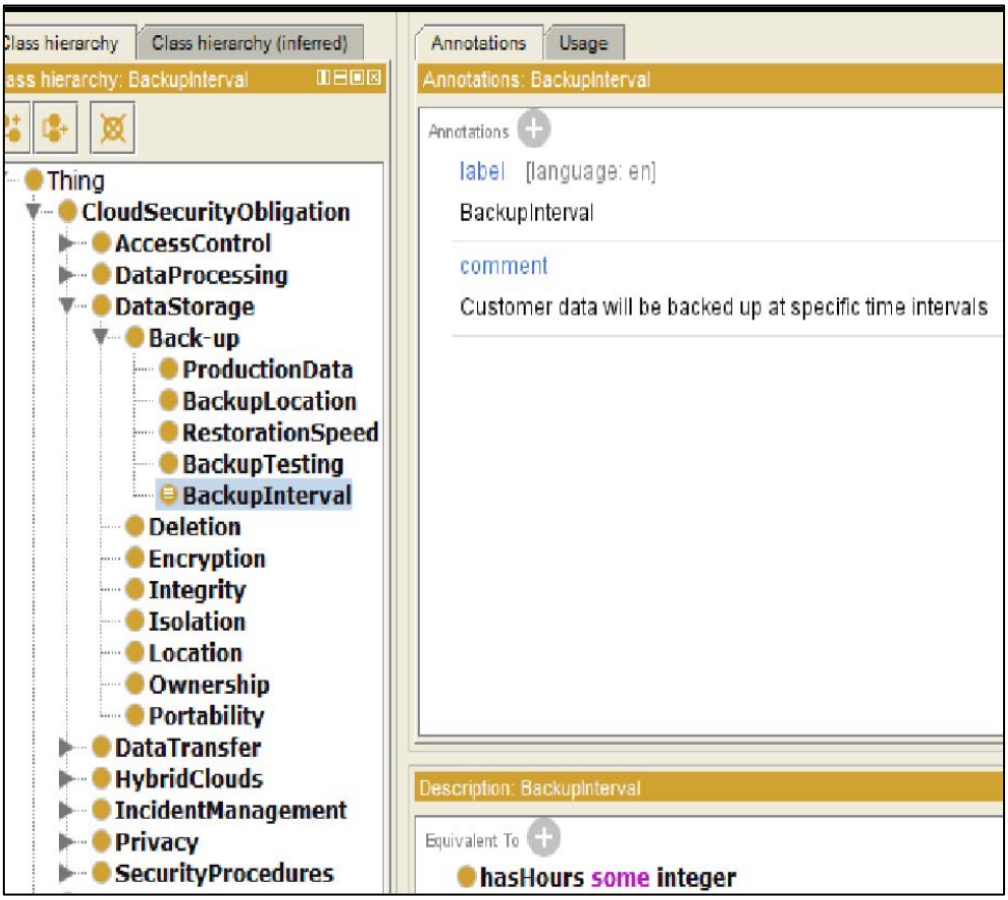


Fig.6. Class Hierarchy in protégé

However, this proposed ontology has many flaws in it, that's why this ontology can be considered as incomplete. The one that is more important flaw is that, this ontology focuses on only security parameters of cloud providers. This ontology does not have any class which ensures security of cloud from outside attacks. Any cloud may be equally vulnerable to attacks from outside the cloud, so it must be made secure from unauthorized access, malicious activity from cloud users etc. so this ontology is incomplete for security of cloud in a sense that it doesn't implement security from *USER*'s side. Moreover, cloud users should also follow certain security obligations like "Terms of Service" etc. but this ontology doesn't provide any class which can check for these obligations

6. Analysis of Ontological Models

A comparative analysis of all these architectures is presented in the following table.

Another issue that should be considered while discussing "Security" is that there are certain Non-technical issues involved in security like reliability, performance of cloud services, risk assessment policies and procedures, management and security governance. Architecture under discussion is unable to address all these non-technical parameters of security as well.

Table 2. Comparative Analysis of All Architectures

Reference of architecture	Models of Cloud Computing reviewed	Objective	Resource monitoring	Assumptions
[1] Ontology for Perception of Network Security State	IaaS, PaaS, SaaS	To monitor the security state of a cloud network, whether it is in safe state or unsafe state	Yes: Actor, Attack, Network, Vulnerability	If location of actor is foreign AND level of automation is automatic AND Goal is to destroy data AND scope is large network AND effected service is more than threshold value then state of cloud network is unsafe or else its state is safe
[2] Ontology for Cloud Security Obligations	IaaS, PaaS, SaaS	To enlist cloud security obligations, necessary for security of cloud computing environment	Yes: Data Processing, Access control, Data Storage, Data Backup	Rules for Data Access, Processing, Data Storage and Backup are defined in terms of ontologies and the above mentioned operations can only be performed if they pass through the ontology specifications
[5] Security Issues in Cloud Computing	IaaS, PaaS, SaaS	To enlist a few basic issues of security in context of particularly cloud computing environment	No	Security of a cloud environment can be depicted in context of Infrastructure security, Network Security and Data security

7. Graphical Representation of Models

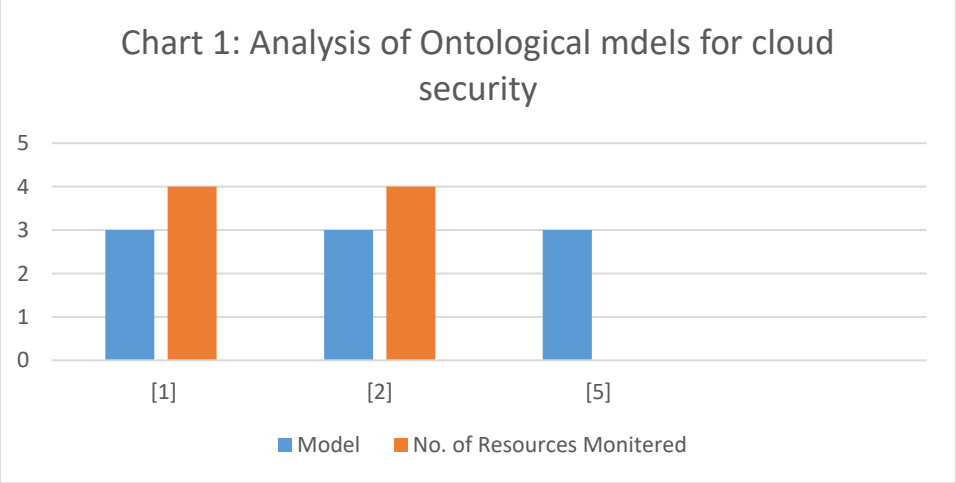
If we compare the efficiency of above discussed models in the form of a graph, the graph will look like as shown in the chart below. In this graph we have shown number of models, number of resources monitored and the efficiency of the proposed ontologies.

All the three ontologies under discussion have covered all the three models of cloud computing i.e., IaaS, PaaS and SaaS.

Second parameter shown in this graph is the number of resources monitored. [1,2] have covered the four, four resources (although their monitored resources are different from each other but total number of resources is equal i.e., 4) while the [5] does not monitor any resource, rather it only enlists a few basic aspects of cloud security, regardless of any particular resource.

Efficiency of the ontologies has been measured on the overall performance of the ontology and the [5] is considered the most efficient one out of these three as its proposed architecture is most efficient in context of detecting threats and vulnerabilities.

The models themselves are discussed in [19]



8. Conclusion

Although all the methodologies we discussed are good enough to provide some mean of cloud security but all of them have some limitations of their own. [1] Does not provide access control mechanism, but the later [2] provides role-based access control. But [2] has its own limitations that it doesn't provide security from user side. It means that any

user is free to show unwanted behavior on cloud, hence violating the Major pillars of security i.e. Confidentiality, Integrity, Authenticity, Availability, Privacy, Trust, Audit and compliance. Similarly [5] also enlisted a few basic security issues of security for cloud but none of the technical issues is addressed in [5] as well. So, a more detailed and comprehensive architecture should be designed which can cover all the aspects of security as security is constantly changing parameter and every day new security threats are being introduced by malicious users.

References

[1] P. Bhandari, M. S. Gujral "Ontology Based Approach for Perception of Network Security State" Proceedings of 2014 RAECS UIET Panjab University Chandigarh, 06 – 08 March, 2014 978-1-4799-2291-8/14/$31.00 ©2014 IEEE

[2] K. Bernsmed, A. Undheim, P. H˚akon Meland, M. G. Jaatun "Towards an Ontology for Cloud Security Obligations" 2013 International Conference on Availability, Reliability and Security

[3] N. F. Noy, McGuinness, D. L., "*Ontology development 101: "A guide to creating your first ontology*". Stanford University, Stanford, CA, 94305, 2001

[4] K. Popović, Ž. Hocenski "Cloud computing security issues and challenges" MIPRO 2010, May 24-28, 2010, Opatija, Croatia

[5] H. Tianfield "Security Issues In Cloud Computing" 2012 IEEE International Conference on Systems, Man, and Cybernetics October 14-17, 2012, COEX, Seoul, Korea

[6] S. Hansman, "*A taxonomy of network and computer attack methodologies".* Supervisor: Ray Hunt, Department of Computer Science and Software Engineering, University of Cantebury, Christchurch, New Zealand, November 2003.

[7] Trend Micro Inc, "Trend Micro's 2012 Global Cloud Security Survey," 2012, http://cloudsecurity.trendmicro.com/ cloud-content/us/pdfs/about/2012 global cloud security survey executive summary.pdf.

[8] G. Hogben and M. Dekker, "Procure Secure: A guide to monitoring of security service levels in cloud contracts," Tech. Rep., 2012, http://www.enisa.europa. eu/activities/Resilience-and-CIIP/cloud-computing/. [Online]. Available: \url{http://www.enisa.europa.eu/activities/ Resilience-and-CIIP/cloud-computing/}

[9] P. Mell, T. Grance "The NIST Definition of Cloud Computing" NIST Special Publication 800-145

[10] "The FedRAMP Security Controls Baseline, version 1.0." 2012, http://www.gsa.gov/portal/category/102371.

[11] Cloud Security Alliance, "CSA Cloud Controls Matrix," Tech. Rep., 2012, https://cloudsecurityalliance.org/research/ccm/.[Online].Available: \url{https://cloudsecurityalliance. org/research/ccm/}

[12] WebCohort, Inc. "Only 10% of Web applications are secured against common hacking techniques", http:/ /2004-feb02.html, 2004.

[13] G. Hulme. "New software may improve application security". http://www.Information week.com, 2001

[14] International Data Corporation, http://blogs.idc.com/ie/wpcontent/uploads/2009/12/idc_cloud_challenges_2009.jpg, 2009

[15] Information Technology Infrastructure Library, http://www.itil-officialsite.com/home/home.asp

[16] International Organization for Standardization, http://www.iso.org/iso/home.htm

[17] Kamta Nath Mishra, "A Proficient Mechanism for Cloud Security Supervision in Distributive Computing Environment", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.6, pp.57-77, 2020. DOI: 10.5815/ijcnis.2020.06.05

[18] Nagesh Shenoy H, K. R. Anil Kumar, Suchitra N Shenoy, Abhishek S. Rao, Rajgopal K T, "Exploring Deep Learning Techniques in Cloud Computing to Detect Malicious Network Traffic: A Sustainable Computing Approach", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.5, pp. 9-17, 2021.DOI: 10.5815/ijwmt.2021.05.02

[19] Manpreet kaur, Hardeep Singh,"A Review of Cloud Computing Security Issues", International Journal of Education and Management Engineering(IJEME), Vol.5, No.5, pp.32-41, 2015.DOI: 10.5815/ijeme.2015.05.04

Authors' Profiles

Ms. Naila Samad Shaikh is a Lecturer and Head of Computer Science Department at Govt. Degree College for Women, Bosan Road Multan, Pakistan. She has a Masters in Science degree in "Information Technology" from "Bahauddin Zakariya University, Multan", Pakistan. She received her "Master of Information Technology" MIT and Bachelor of Science in Mathematics and Statistics from "Bahauddin Zakariya University Multan", Pakistan. Her research interest includes Cloud Computing, cloud security, Web semantics, cyber security and Internet security.

Affan Yasin received his Bachelor of Science in Computer Science (BSCS) from National University of Computer, and Emerging Sciences (NUCES-FAST), Lahore, Pakistan, and he has received his Master of Science in Software Engineering (MSSE) degree from Blekinge Tekniska Högskola (BTH), Karlskrona, Sweden. Recently, he has completed his Ph.D. under the supervision of Prof Jianmin Wang and Associate Professor. Lin Liu at Tsinghua University, Beijing, P.R.China. His area of interest includes empirical research and development within Software Engineering, game-based learning, social engineering, serious game, and requirements engineering. Currently, he is working as a Post-Doctoral researcher at Tsinghua University, Beijing, P.R.China.

Rubia Fatima received her Master's degree in Information Technology (MSIT) from Bahauddin Zakariya University (B.Z.U), Multan, Pakistan. Currently, she is doing her PhD under the supervision of Prof Jianmin Wang and Associate Professor. Lin Liu at Tsinghua University, Beijing, P.R.China. Her area of interest includes empirical research and development within Software Engineering, game based learning, social engineering, cyber security, information security, serious game and requirements engineering.

How to cite this paper: Naila Samad Shaikh, Affan Yasin, Rubia Fatima, "Ontologies as Building Blocks of Cloud Security", International Journal of Information Technology and Computer Science(IJITCS), Vol.14, No.3, pp.52-61, 2022. DOI: 10.5815/ijitcs.2022.03.05

