A Comparative Study of Cloud Security Ontologies

Vaishali Singh
Department of Computer Science,
St. Xavier's College, Jaipur, India
vaishali.siingh@gmail.com

S. K. Pandey
Department of Electronics & Information Technology
Ministry of Communications & IT,
Government of India, New Delhi, India
santo.panday@yahoo.co.in

Abstract— **Cloud Security is one of the foremost concerns among related stakeholders. Each concern brings diverse effects on discrete assets while analyzing the security issues in Cloud Computing. In spite of various studies, we still fail to define the needs of security, resulting in a slow pace in cloud adoption. Accordingly, a fresh approach is required to facilitate end-users and service providers to better understand the domain so that they can easily address their security requirements and find their solutions. Out of different security measures used by related stakeholders one is 'ontology-based security approach,' which creates a conceptual relationship among entities representing information, having systematic review for the purpose of identifying, analyzing and eliciting security countermeasures. Previous studies reveal a variety of security ontologies that can be used by the service providers, which have different approaches to assess the security; still, cloud service providers and end users find it complicating and lacking in security sphere as there is no specification, which ontology should be used at what condition. Hence, there is an emergent need for a critical review of prior studies related to Cloud Security Ontology. This paper presents a brief discussion on five major ontologies namely: Cloud Ontology, Takeshi Takahashi et al.'s Ontology, CoCoOn, Subramani Keerthana et al.'s Ontology and Nelson Gonzalez et al.'s Taxonomy dwelling upon their strengths and weaknesses. A comparative study is also accomplished using various attributes, which are identified based on the well-known practices with similar studies in security domain. Further, future research directions based on comparative study and the weaknesses sections have also been explored to facilitate the researchers in related areas.**

Index Terms— **Cloud Computing, Security Ontologies, Cloud Security Ontologies, Comparative Study.**

I. INTRODUCTION

Now-a-days, cloud security has becomes a very vibrant issue in the computing world [1]. One major area on which the modern era business depends is outsourcing of computational services and resources, which is speeding up due to progressive Cloud Computing [1]. On-demand services and virtualization of centralized data and resources through the internet have made life faster and easier [1]. But along with the rapid growth, cloud service is responsible among service providers and customers for various security issues and multifarious threats. One of our prior studies had already provided a comprehensive review of existing literature of Cloud Computing [2]. It highlighted several issues and challenges particularly relating to cloud security [3] [4].

It is a difficult to answer simple questions like 'Are you secure to use cloud?' or 'What is needed to be invested to get secure?' When organization assets get connected with the outer world, they are susceptible to damages through exploiting vulnerabilities by threats and attacks [5]. Ontology is one such related approach used to determine the relationship between the entities having methodical review for the purpose of analyzing security countermeasures [6]. Security countermeasures are such investments that use the ontology for overall security measurement, which could help in security supervision. The deficiency of knowledge about the domains, assets, threats and possible countermeasures of security result in wrong decisions [7]. There are a number of reasons for this; one of them is undefined security terminology.

There are many methods to assess the security but are not found to be so effectual due to rising intricacy of vulnerabilities and threats. Prior research studies depict that there is no comprehensive comparative study, which shows the strengths and weaknesses of all major security ontologies related to cloud that will assist organizations in determining, which countermeasures is the best, in terms of Cloud Computing. One major objective is to compare and analyze the same along with their respective strengths and weaknesses and propose future research directions that may help researchers to develop a new ontology with respect to cloud security. The study may also provide awareness about imperiling threats, assets and security objective, which reduce the prospect of damage.

Apart from the above introduction on background points, remaining paper is organized as follows: Section II demonstrates 'Ontology' with respect to security. Section III presents a brief discussion of the 'Existing Security Ontologies' related to cloud, whereas in Section IV, 'Strengths and Weaknesses' of each one is discussed. In Section V, a 'Comparative Study' is done on the basis of the critical review. Section VI presents 'Future Research Directions' in the area and 'Conclusion and Future Work' are reported in Section VII.

II. ONTOLOGY

"Ontology" can be defined as an explicit act of describing concepts (classes) in a disclosure domain with reference to the characteristic of each concept (class) elaborating its various features, attribute and roles, as well as facets and role restrictions [8]. It can be said that Ontology is an overall collection of entity instances of the classes, which compose a base for knowledge [8]. In other words, an ontology contains classes that represent concepts organized in taxonomies to define superclass-subclass hierarchy; relations that represent association between concepts; attributes to describe the features of the concepts; functions are special case of relations; instances that signify elements in an ontology [9].

978-1-4799-6896-1/14/$31.00 ©2014 IEEE

Development of the security based ontology render an ontological composition for knowledge based security domain. The security ontology formalizes security knowledge considering threats, vulnerabilities, controls, and their interdependencies which is constructive to find countermeasures [10]. Ontology will provide cloud security a base for contributing towards general perceptive of the structure of information among cloud service providers and users, reusability of domain knowledge, explicit development of domain assumptions, differentiation between knowledge based domain from the knowledge based operation and analytical study of knowledge based domain.

III. EXISTING ONTOLOGIES SURVEY

Various cloud ontologies are reported in prior research [12] [13]. However, a comprehensive study was needed to analyze the existing contributions, which are significant and emerge valuable among all. Some of the selections, from the trend-setting research contributions in the related area have been briefly explained for scrutiny of strengths and weaknesses.

3.1 Cloud Ontology

The research study analyzed that the Cloud Computing is an effective resource management platform with two major types: public and private. It depicted that the private cloud is more secured as it is formed within the organization so that only authorized users can access the resources; but in case of public, data is shared among all the cloud users, so security emerges as a major issue [26]. To improve security issue, data is outsourced to the third party storage but still it is a challenging task. For this researchers accomplished a detailed study about the cloud and also highlighted that it can be used in cloud to improve security on the outsourced data. It represented the layered ontology of cloud, which showed the inter relations and inter dependency between the layers [26].

Researchers used encryption through public key cryptography for cloud security. A detailed study about auditing mechanism was explained by monitoring data and maintaining the log records for improving the protections of the cloud data. The researchers also studied identity-based encryption and suggested one of the identities to achieve authentication as well as confidentiality. Accordingly, they concluded that using three methods, i.e. encryption, auditing, identity means definitely, one can successfully achieve cloud security without any threats [26].

3.2 Takeshi Takahashi et al.'s Ontology

This ontology gave a holistic view of cyber security operational information clarifying what type of incident log will be as well as 'what type of asset description information was needed for each user organization in Cloud Computing' [11]. Researchers discussed 3 important components that influence information of cyber security in Cloud, i.e. data-asset decoupling, multiple resources composition and external resource usage [27].

Based on changes in Cloud Computing, they have identified the necessity of cyber security information raised due to data provenance and dependency of resource information [11]. They concluded the availability is the most important concern. Further, they also identified the entities and defined the domains for cyber security operations, which were required to run the operations to build the ontology of cyber security [11].

3.3 CoCoOn

The study presents Web Ontology Language (OWL) based ontology known as the Cloud Computing Ontology (CoCoOn). This ontology explained the functional and non-functional concepts, attributes and relations of IaaS (Infrastructure as a Service). The CoCoOn also specified the domain model of the IaaS layer. This ontology elaborated the explanation of cloud infrastructure services. The study facilitated the innovation of infrastructure services based on functionality and Quality of Service (QoS) parameters through mappings from provider descriptions [14].

The ontology established domain classification to describe specific aspects of Cloud Computing for guiding reference. It was built upon the Web Service Modeling Ontology (WSMO) and standard semantic Web Ontology Language Service (OWL-S), which had layered ontology on the top of web service models [28]. Accordingly, the grounded model and process model of OWL-S amalgamate with cloud ontology to concisely express infrastructure services by modelers [14].

The study was mapped with the most prominent set of infrastructure services (i.e. Amazon, Azure, GoGrid, Rackspace, etc.) to CoCoOn. In the CoCoOn, all the common metadata fields were included such as organization, author and first name, etc. referenced through standard web ontologies. The CoCoOn consisted of two parts: functional cloud service configurations information parameters and non-functional service configuration parameters [14].

3.4 Subramani Keerthana et al.'s Ontology

The proposed Ontology in Cloud Computing explained the Ontology based Inter Cloud Directories and Exchanges undergoing in depth of Inter Cloud Topology, Ontology-Based Cloud Computing Resource Catalogue and Ontology-based Intelligent Customization Framework for SaaS [25]. The researcher concluded that ontology had an important role in cloud technology. The research study explained unique attributes required for assessment in fields such as recovery, data integrity, privacy and legal consequences, which resulted in the depiction that security was a major issue in clouds [25].

Afterwards, researchers proposed to figure up a security model for an application access control in cloud using 'Ontology DB', 'Reference Ontology', 'Ontology Comparator', 'Context Collector', 'Role Evaluator' interacted with the databases and role and access policy, policy databases to determine the security level. 'Policy Controller' included granting, denying or revoking access to various services [25]. The resulted security service was accepted by the service model and the operations were performed according to the security checking process.The research analyzed the importance of ontology in the Cloud Computing by amalgamating a view of computing assets existing across different clouds, providing the capability to secure sensitive

data from unauthorized access and by enhancing the overall efficiency [25].

3.5 Nelson Gonzalez et al.'s Taxonomy

The study on Cloud Computing security taxonomies aimed to classify, identify, quantify, and organize the security concerns, to find countermeasures linked to Cloud Computing. The study focused on issues, which were specific and distributed in Cloud Computing environment [15]. Research provided an improved check of the Cloud Computing security taxonomy, which were previously presented in the literature.

Further, researchers analyzed the security aspects linked to virtualization in Cloud Computing. Finally, security taxonomy was proposed, which highlighted three major categories: privacy, architecture and compliance related to security [16] [19].The work identified and grouped the main problems into seven categories forming a model. These aforementioned categories are: Legal issues, security based Network, Virtualization, and security of data, Governance, Interfaces and Compliance [15]. These categories had numerous prospective security problems, which resulted in a categorization with subsection of the chief issues recognized above. A valued approach was applied to recognize the quantity of references associated to each category [15].

IV. STRENGTHS AND WEAKNESSES

After a critical review of the above mentioned ontologies, major strengths and weaknesses have been identified, which are given as follows:

4.1 Cloud Ontology

Major strengths and weaknesses relating to the Cloud Ontology are given as follows:

a) Strengths: The key strengths are as under:

- The detailed study about security issues in Cloud Computing had been done with the layered ontology of Cloud Computing, which showed the inter dependency and inter relations among the layers.
- The study explained the security methods using encryption for cloud security with the help of Public Key Cryptography.
- Overall, the study depicted that using three methods i.e. encryption, auditing, identity means definitely one can successfully achieve cloud security without any threats.

b) Weakness: These are as follows:

- This ontology is based on the prior opinions, which could have over-looked recent developments hence; the need to quantify a maximum number of steps is a key weakness.
- Threats and vulnerabilities are not significantly focused in the given ontology. Hence, further work may be done in this direction to increase the security level.
- Attributes like Confidentiality, Integrity, Availability and Non-Repudiation must be taken into consideration for improvement of security assessment [20].
- A deeper study is needed to identify the threats and countermeasures for the service providers to improve high levels of security conformity for clouds.

4.2 Takeshi Takahashi et al.'s Ontology

An analytical study of the ontology reveals some strengths and weaknesses, which are given in the following sections:

a) Strengths: These are as under:

- It presented a holistic view of cyber security operational information relevant to incident log and type of asset description information, which was needed for each organization in Cloud Computing.
- 3 important components that involve cyber security data in Cloud Computing i.e. data-asset decoupling, multiple resources composition and extraneous resource usage were considered appropriately.
- Based on the changes in Cloud Computing, researchers also considered the necessity of cyber security information raised due to data provenance and dependency of resource information.

b) Weaknesses: These are as follows:

- This ontology is also based on the prior opinions, which could have over-looked recent developments hence; the need to quantify a maximum number of steps is an essential requirement.
- Threats and vulnerabilities are not significantly focused in the given ontology. Hence, further work may be done in this direction to increase the security level.
- Besides attributes like preservation of information Confidentiality, Integrity, Availability, and many other features like Non-Repudiation can also be included which have been left unidentified [20][21].
- Common Vulnerabilities and Exposures (CVE) [22] can be used to describe vulnerability's impact range, but no mechanism is used to measure the impact of vulnerability.
- There may be many other factors besides decoupling of data-asset, multiple resources composition and extraneous resource utilization, which have also not been considered.

4.3 CoCoOn

A detailed study of CoCoOn reveals some strengths and weaknesses, which are given in the following section:

a) Strengths: The major strengths of CoCoOn are reported as under:

- The ontology defined and facilitated the domain model of the IaaS layer and description of Cloud infrastructure services in a proper way.
- It facilitated the discovery of infrastructure services based on their functionality and Quality of Service (QoS) parameters.
- It presented the parts of the ontology in a visual form produced by the Cmap Ontology Editor tool.
- Ontology was divided into functional cloud service configurations information parameters; and non-functional service configuration parameters.
- It mapped the most prominent set of infrastructure services (i.e. Amazon, Azure, GoGrid, Rackspace, etc.) to CoCoOn.

b) Weaknesses: The major weaknesses of CoCoOn are given as follows:

- The ontology is based on prior opinions, which could have over looked recent developments; hence, the need to quantify a maximum number of steps is required at this moment.
- CoCoOn is a generalized one; hence, the need for expansion of the research particularly towards security requirements is still needed.
- This is based on IaaS model only; there is no discussion on SaaS and PaaS.
- Threats and vulnerabilities are not significantly attended to in the given ontology. Hence, further work may be done in this direction to increase the security level.

- CoCoOn does not clearly talk about the security attributes, e.g. Confidentiality, Integrity, Availability and Non-Repudiation, etc. [20]. This too has to be taken into consideration.

4.4 Subramani Keerthana et al.'s Ontology

A critical study of this ontology reveals some strengths and weaknesses, which are given in the subsequent sections:

a) Strengths: The key strengths are as under:

- Ontology consolidated the view of computing resources presented across different clouds providing ability for protection of sensitive information from unauthorized access, customization of SaaS and improvement of overall efficiency.
- The study explained those unique attributes required for assessment in fields such as recovery, privacy, legal issues and data integrity concluding security is a major issue in cloud.
- It figured up a security model for application access control in cloud using 'Ontology DB', 'Reference Ontology', 'Ontology Comparator', 'Context Collector', 'Role Evaluator' and 'Policy Controller'.

b) Weaknesses: The key weaknesses are as follows:

- This ontology is also based on the prior opinions, which could have over looked recent developments hence, the need to quantify a maximum number of steps is the demand of the day.
- Threats and vulnerabilities are not significantly focused on the given ontology. Hence, further work may be done in this direction to increase the security level.
- Three primary studies: intelligent ontology based registers, intelligent customization framework for SaaS (Software as a Service), and design of security system used in Cloud Computing are insufficient and could be more deeply elaborated in other area/s also.
- Attributes like Confidentiality, Integrity, Availability and Non-Repudiation must be taken into consideration for improvement of security assessment [20].

4.5 Nelson Gonzalez et al.'s Taxonomy

The major strengths and weaknesses relating to the Taxonomy are given as follows:

a) Strengths: The key strengths are given below:

- The study aims to classify identify, quantify and organize security concerns to find countermeasures.
- It provided an improved check of the Cloud Computing security taxonomy in the previously presented literature with an in-depth analysis of the major security frameworks (National Institute of Standard and Technology (NIST) and Cloud Security Alliance (CSA), European Network and Information Security Agency (ENISA))[16] [17][18].
- Further, the security aspects linked to virtualization in Cloud Computing have also been addressed.
- The study presented security issues and solutions via pie charts through demonstration of each category in the full amount of references keyed.
- Taxonomy identified a number of solutions, addressing each concerned category/group using radar graph.
- It analyzed the cloud trend revealing a significant amount of security concern, solutions and best practices, which had been well studied and developed.

b) Weaknesses: The key weaknesses are as follows:

- This Taxonomy is also based on the prior opinions, which could have over looked recent developments; hence, the need to quantify a maximum number of steps is currently required due to advancement in technology.
- It is a generalized one; hence, the need for extension of the research particularly towards security requirements is still needed.
- Threats and vulnerabilities are not significantly focused in the given ontology. Hence, further work may be done in this direction to increase the security level.
- Cloud security taxonomy highlighted limited security attributes related to privacy, architecture and compliance; hence, more security attributes are required to be included.
- Several consequences still need further research attempt, especially those, which are associated to secure virtualization.
- In depth study is needed to identify threats and countermeasures for the service providers to improve high degree of security compliance for clouds.

V. COMPARATIVE STUDY

For accomplishing a comparative study of the aforementioned ontologies, some attributes have been identified based on the well known practices with similar studies. These are described as follows:

- **Well-defined ontology with appropriate design and methodology:** The ontology should be a formal, explicit specification of an abstract model of distinct phenomenon with identified relevant concepts shared by a group of knowledgeable domain [9]. The methodological process of ontology should decide the domain and the purpose of the ontology; sources: documents and existing ontologies [9]. Ontology should be divided into modules e.g. basic core module, security and reliability module and security requirements module [9].
- **Ontological specification of security requirements:** Gathering and analysis of requirements for the ontology is necessary. As a result, Ontology Requirement Specification Document (ORSD) is created based on technical requirements,quality requirements and other requirements needed by the client of the ontology [23] [24]. The requirement should specify concepts, entities, classes and relations among the classes; organize in a taxonomy form; discuss on inheritance issues among super class-sub class; evaluate the attributes and instances, which are real elements in our domain [9].
- **Incorporation of security attributes in totality**: Confidentiality, Integrity, Availability and non repudiation are the basic pillars of cloud security. Preservation of all aforementioned attributes must be considered in any process [21].
- **Analysis of threats and vulnerabilities**: The weaknesses of the software are known as vulnerabilities, which result in threats. There are a range of wide-reaching databases, which preserve the catalogue of these vulnerabilities along with their countermeasures. Therefore, it is imperative to address the same in the ontology.
- **Security Countermeasures and Controls:** Controls should be provided on the basis of security ontology to extenuate an distinguished threats, vulnerability and to protect the respective assets by corrective, preventive, deterrent, detective or recovery measures (control type) [9].
- **Validation & Evaluation**: Security ontology should be precise, consistent, complete and concise. It needs to be

supported by live projects illustrations. The ontology should have trust level and the level of usability, which is relevant to standard compliance.

On the basis of the review results, i.e. strengths and weaknesses, a comparative study of the above mentioned ontologies is done hereby.

Table 5.1 is made for the comparative study at-a-glance. If ontology fully satisfies an attribute, a mark √ is drawn against the column, otherwise × is marked.

TABLE I. COMPARISON OF SECURITY ONTOLOGIES

Attributes	Cloud Ontology	Takeshi Takahashi et al.'s Ontology	CoCoOn	Subramani Keerthana et al.'s Ontology	Nelson Gonzalez et al.'s Taxonomy
Well-defined ontology with appropriate design and methodology	√	√	√	√	√
Ontological specification of security requirements	√	√	×	×	√
Incorporation of security attributes in totality	×	×	×	×	×
Analysis of threats and vulnerabilities	×	√	×	×	√
Security Countermeasures and Controls	×	√	×	×	×
Validation & Evaluation	×	√	×	×	√

VI. FUTURE RESEARCH DIRECTIONS

In the light of the above discussion, some future research directions have been identified, which are given as follows:

- **Cloud Ontology** made a detailed study about the cloud and how it can be used in cloud to improve security on the outsourced data and represented the layered ontology of cloud, which showed the inter-relations and inter-dependency between the layers. Future research may be done throwing light on the significance of security necessities having all suitable security attributes for finding mitigation techniques of threats and vulnerabilities.
- **Takeshi Takahashi et al.'s Ontology** has focused on cyber security information in Cloud Computing, but not focused on threats and vulnerabilities related to Cloud Computing. Future work may be initiated to add vulnerability, threats and their mitigation techniques.
- **CoCoOn** revealed that the same is not focused on IaaS security requirements, threats, vulnerability and countermeasures. In addition, functional and non-functional concepts, attributes and relations are also needed to be proposed for other service models such as Platform as a Service and Software as a Service. Further direction is to consider more security attributes like Confidentiality, Integrity, Availability (CIA) and Non-Repudiation, etc. to enhance the security levels in cloud and to detect suitable countermeasures.
- **Subramani Keerthana et al.'s Ontology** revealed that there is not enough focus on the major security attributes. Moreover the study focused on access control and authorization technique only. Research may be done throwing light on the importance of security requirements having all appropriate security attributes for finding mitigation techniques of threats and vulnerabilities.
- **Nelson Gonzalez et al.'s Taxonomy** highlighted 3 major categories: security related to architecture, privacy and compliance arranged in hierarchical form. Further research may be undertaken for developing cloud security ontologies incorporating security attributes in totality and evaluating the concepts and the taxonomies, attributes and relations for finding out the appropriate countermeasures required.

VII. CONCLUSION AND FUTURE WORK

Research community has made significant progress on many fronts in the area of cloud security. At the same time, demands placed on Cloud Computing and the security issues have increased significantly raising numerous crucial research questions. The paper presented a comparative study, of the strengths and weaknesses of the existing security ontologies related to Cloud Computing together with future research directions. It is evident that still there is a need to develop a cloud security ontology having all the appropriate attributes.

Future work may be initiated towards addressing the issues identified in the weaknesses section of any of the ontology discussed in the paper. Moreover, a new ontology may also be proposed addressing all the related aspects. The paper will help the related stakeholders to establish better protection in the cloud environment.

REFERENCES

[1] Southern African Internet Governance Forum (SAIGF), "Emerging issues - Cloud Computing", Issue Papers No. 1. http://www.apc.org/en/system/files/1.CloudComputing.pdf

[2] Vaishali Singh & S. K. Pandey, "Research in Cloud Security: Problems and Prospects", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) Vol. 3, Issue 3, Aug 2013, pp. 305-314.

[3] Vaishali Singh & S. K. Pandey, "Revisiting Cloud Security Issues and Challenges", International Journal of Advanced Research in Computer Science and Software Engineering Vol.3.Issue7, July-2013, pp. 1-10.

[4] Vaishali Singh & S. K. Pandey, "Cloud Security Related Threats", International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 pp. 2571.

[5] Network Security 1 and 2 Companion Guide, "Vulnerabilities, Threats, and Attacks", chapter 1, http://ptgmedia.pearsoncmg.com/images/1587131625/samplechapter/1587131625content.pdf

[6] Vaishali Singh & S. K. Pandey, "Revisiting Security Ontologies", IETE Technical Review Journal, Taylor & Francis Online, submitted.

[7] AnoopSinghal&DumindaWijesekera, "Ontologies for Modeling Enterprise Level Security Metrics", CSIIRW '10, April 21-23, USA

[8] Natalya F. Noy and Deborah L. McGuinness, "Ontology Development 101: A Guide to Creating Your First Ontology", http://www.ksl.stanford.edu/people/dlm /papers/ontology101/ontology101-noy-mcguinness.html

[9] Julita Bermejo, "A Simplified Guide to Create an Ontology",ASLab R-2007-004 v 0.1 Draft May 22, 2007

[10] Stefan Fenz. “Security Ontology” http://stefan.fenz.at/research/security-ontology/

[11] Takahashi Takeshi, YoukiKadobayashi, Hiroyuki Fujiwara, “Ontological approach toward cybersecurity in Cloud Computing”, Proceedings of the 3rd international conference on Security of information and networks, 2010-09-07, pp. 100-109.

[12] DarkoAndrocec, NevenVrcek, JuricaSeva. “Cloud Computing Ontologies: A Systematic Review”, MOPAS 2012 : The Third International Conference on Models and Ontology-based Design of Protocols, Architectures and Services, pp. 9-14

[13] C. A. Martinez, G. I. Echeverri, and A. G. C. Sanz, ―Malware detection based on Cloud Computing integrating Intrusion Ontology representation, 2010 IEEE Latin-American Conference on Communications (LATINCOM), pp. 1-6, September, 2010.

[14] Miranda Zhang, Rajiv Ranjan, Armin Haller, DimitriosGeorgakopoulos, Michael Menzel, Surya Nepal, “An Ontology-based System for Cloud Infrastructure Services’ Discovery”, CollaborateCom, pp. 524-530. IEEE, (2012)

[15] Nelson Gonzalez, Charles Miers, Fernando Red´ıgolo, Marcos Simpl´ıcio, TerezaCarvalh, Mats N¨aslund and MakanPourzandi, “A quantitative analysis of current security concerns and solutions for cloud computing”, Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012, 1:11

[16] CSA (2009) Security Guidance for Critical Areas of Focus in Cloud Computing. Tech. rep., Cloud Security Alliance

[17] Catteddu D, Hogben G (2009) Benefits, risks and recommendations for information security. Tech. rep., European Network and Information Security Agency, enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment

[18] Mell P, Grance T (2009) The NIST Definition of Cloud Computing. Technical Report 15, National Institute of Standards and Technology, www.nist.gov/itl/cloud /upload/cloud-def-v15.pdf

[19] Mather T, Kumaraswamy S (2009) Cloud Security and privacy: An Enterprise Perspective on Risks and Compliance. 1st edition. O’Reilly Media

[20] S. K. Pandey, K. Mustafa, “Security Assurance by Efficient Non-repudiation Requirements”, Proceedings of the Second International Conference on Computer Science, Engineering & Applications (ICCSEA 2012), May 25-27, 2012, New Delhi, India. Volume 2 pp. 905-912.

[21] Mustafa K, Pandey S K, Rehman S. Security assurance by efficient access control and rights. CSI Communication. September, 2008; 32(6): pp. 29-33.

[22] Common Vulnerabilities and Exposures, The Standard for Information Security Vulnerability Names,Cybersecurity and Communications, U.S. Department of Homeland Security. The MITRE Corporation.

[23] Tomasz Boi´nski, PiotrOrłowski, Julian Szyma´nski and HenrykKrawczyk “Security ontology construction and integration”, International conference on knowledge enginerring and ontology development, 2011.

[24] Asunción Gómez Pérez, Mari Carmen Suárez de Figueroa Baonza, Boris Villazón, “NeOn Methodology for Building OntologyNetworks: Ontology Specification” pp.1-18

[25] KeerthanaSubramani, PriyaDharshiniPonniahRajagopal, SavithaSundaramoorthi, “Ontology in Cloud Computing”, http://cloudontology.wikispaces.asu.edu/Use+of+Ontology+in+Cloud+Computing#Use Of Ontology In Cloud Computing-Design of Security System [Accessed: 19-02-2014].

[26] E.Kamalakannan, B.Prabhakaran, K.S.Arvind, “A Study on Security and Ontology in Cloud Computing” International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2013.

[27] Bhraguram, T.M, and M.S Sumesh. "Cyber security information exchange based on Data Asset De-coupling factor in cloud computing", 2011 IEEE Recent Advances in Intelligent Computational Systems, 2011.

[28] Bo Hu. "Research on the Application of RGPS Domain-Based Requirements Elicitation and Analysis for Web Service Discovery", 2009 Fifth International Conference on Semantics Knowledge and Grid, 10/2009

AUTHORS

Vaishali Singh is presently working as an Assistant Professor in the Department of Computer Science, St. Xavier’s College, Jaipur, India. She has an excellent academic background right from the school level. Under the Institute-Industry linkage program, she delivers expert lectures on various areas of Computer Science. She has contributed three research papers in reputed International journals and national conferences. Her research interest includes: Cloud Security, Cloud Security vulnerabilities, threats and countermeasures, Access control, Identity measurement etc.

Dr. Santosh K. Pandey is presently working as Scientist 'C' with the department of Electronics & Information Technology, Ministry of Communications & IT, Government of India New Delhi. Before joining DeitY he was a Faculty of Information Technology with Board of Studies, The Institute of Chartered Accountants of India (Set up by an Act of Parliament) New Delhi. Prior to this, he worked with the Department of Computer Science, Jamia Millia Islamia (A Central University) New Delhi and Directorate of Education, Govt. of NCT of Delhi. He has a rich Academics & Research experience in various areas of Computer Science. His research interest includes: Software Security, Requirements Engineering, Security Policies and Standards, Formal Methods, Cloud Computing, Security Metrics, Vulnerability Assessment etc. He has published around 46 high quality research papers and articles in various acclaimed International/National Journals (including IEEE, ACM, CSI) and Proceedings of the reputed International/ National Conferences (including Springer). Out of these publications, most of them have good citation records. He has been nominated in the board of editors/reviewers of various peer-reviewed and refereed Journals. In addition, he has also served as a Program Committee Member of several reputed conferences in India as well as abroad. He has also been designated in various academic/research committees by the government organizations as well as software companies as a subject experts.