Revisiting Security Ontologies

Vaishali Singh
Department of Computer Science,
Jagannath University, Jaipur, India

S. K. Pandey
Department of Electronics & Information Technology
Ministry of Communications & IT, Government of India
New Delhi, India

***Abstract*— Contemporary exploration of all stages of service models clearly proves the immense significance of "Security in Cloud Computing", which being as obtuse as it is pertinent, demands attention. An analysis of recent studies depicts certain useful approaches for the fulfilment of security objective; however, these advancements are largely inconsistent with the forays of research in other fields. Numerous technologies amalgamate in the implementation of cloud computing security, one of which is ontology. In this paper, a critical study of security ontologies has been accomplished in which these ontologies have been further classified into three major categories: Generalized, Specific with sub categories: Web Services (WS) and Web Ontology Language (OWL) based Security Ontologies, Network Security Ontologies, Security Requirements Ontologies, Risk based Security Ontologies and Application based Security Ontologies; and Miscellaneous. The present research aims to firstly, classify the above-said ontologies and thereby offer a prismatic analysis of the same. By using ontology, one can aim at securing the cloud through security countermeasures with consideration of applicable threats and security solutions deployed to support appropriate security services and objectives.**

Keywords—Cloud Computing, Security Ontology, Cloud Security, Cloud Security Ontology**.**

I. INTRODUCTION

Significant innovations in virtualization and distributed computing as well as improved access to high-speed Internet have induced interest in Cloud Computing [1]. Cloud Computing is a vast area or terminology and it involves delivering hosted services over the Internet containing scalability, abstracted infrastructure, virtualization, on-demand access, connectivity, resource pooling, elasticity, and pay-per-use utility model [2].

Acquiring of cloud services depends upon delegation of responsibilities among the service providers, the customers and it is interlinked with security issues viz. reliability, availability of services and data, complexity, costs, performance, migration, reversion, regulations and legal issues and the lack of standards [2]. Along with the large-scale use of virtualization in implementing Cloud, infrastructure also plays an important role in the Cloud services.

Security for cloud computing has gradually developed into a very large field of research. Contrary to the past, Cloud data assurance and their security, trust, privacy have moved up the ladder and are being considered by the cloud service provider, stakeholder etc. as a subject of interest to become cloud research issues. Bringing to the mind that cloud security allows fabricating basic concept of reliable systems, which faces threats, errors and attacks via several origins: technical origin, intentional origin, accidental origin and natural origin.

It is important to create trust bonds between the providers and clients; security does this in terms of software services. Proper implementation of security mechanisms can eliminate most of the vulnerabilities [3]. Security mechanisms have a set of objectives to reduce the extent of vulnerabilities like authentication, access controls and rights, confidentiality, non-repudiation etc. [4] [5] [6]. The basic concept strives to protect data through a set of techniques and methods [5]. Likewise security will be ensured for deployed software by non-repudiation which will be enforced in the security objective and this will provide additional measures for security assurance [7].

The intention of the attacker is to acquire the assets by exploiting vulnerability leading to safety failure; the security mechanism theory therefore, depends on the attackers' mindset. Despite all the prior methodologies, there is still the need for a generalized setup of security requirements and terminology in the terms of ontology for cloud computing. The representation of an interrelated concept in the field of knowledge is ontology.

Various security ontologies have been reported in the literature. Accordingly, a brief but complete description of the reported ontologies has been presented in the paper along with the related discussion as conclusive points. However, the ultimate aim is building ontology for security operational information, based on the threats included in cloud from the source, origin and attack to its countermeasure.

Beyond this introduction on the background details, the remainder of this paper is structured as follows: Section II describes "Security Ontologies" and Section III presents "Related Work" by the researchers in the area. Section IV provides the "Analysis of Reported Ontologies" along with related discussions. Finally, "Conclusion and Future Work" have been reported in Section V.

II. SECURITY ONTOLOGIES

Ontology is the operational model of entities and relationships in a specific domain of knowledge [8]. Security ontologies are ways to define security terminology, by removing the conflict among the security experts and the customers; they precisely define the entities and their relationships to each other. There is a standard block of risk analysis: assets, threats, vulnerabilities and countermeasures in the security ontology model, these four components are the basic building blocks of security and their relations [9]. The description of each block with technical concepts results in an ontology having a classification and definition of specific domain vocabulary.

Security relationship model is the foundation to develop the security ontology, which is explained by the National Institute of Standards and Technology (NIST) Special Publication 800-12 [10]. The conceptualized high level relationships between the entities are shown below in Fig 2.1.

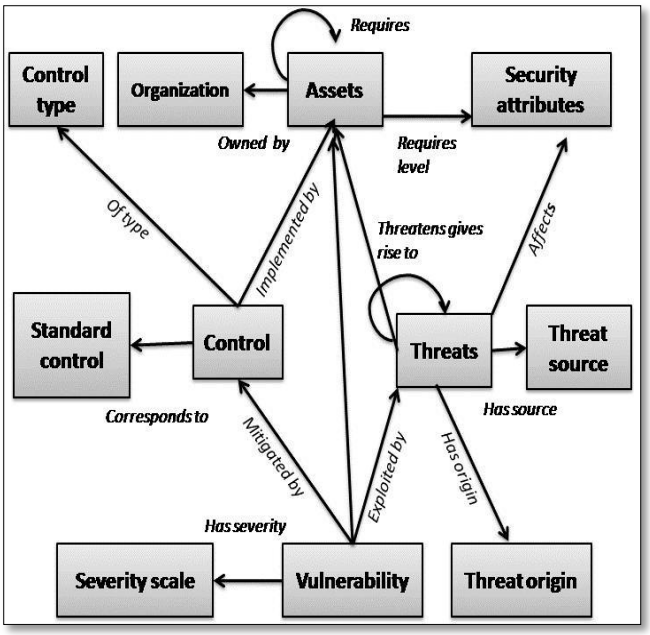

Fig.2.1: Relationship among Security Related Terms (Source [10])

A distinct threat gives rise to other threats, which forebodes the forthcoming hazard to an organization and its assets [10]. These threats influence the security objectives (integrity, confidentiality and availability) in the form of a physical, administrative and technical weakness as vulnerability. Threats can be natural or human origin using accidental or deliberate source [10].

The asset on which the weakness could be subjugated is assigned. Different control types such as preventive, deterrent, recovery, corrective and detective measure controls need to be implemented on the vulnerability to protect the assets. By the incorporation of widely accepted knowledge and best–practice information security standards, the derived controls are insured. The controls are reusable for different standards as modelled on high granular levels [10]. In the prior research, various attributes were identified and followed the risk assessment steps for security assurance in the earlier stage of development lifecycle [11].

Several issues and challenges have already been highlighted [13], for which the study has already provided a detailed cloud security review of the existing literature [12] particularly relating to Cloud security that decreases its adoption rate and resulted to identify the major security threats [14]. Some of the security solutions deliver integrated and automated features for the clear visibility in entire cloud system to sustain compliance [15].

But still, there is a need to find the appropriate countermeasures for these attacks and threats, there appears a need to develop the cloud security ontology. The next section will cover the related work reported in the literature on security ontologies.

III. RELATED WORK

Undergoing research concluded that there are a few related works that focus on expanding security ontology for a generalized base for the growth of cloud applications. This section highlights already accomplished research contributions available in literature. The reported ontologies have been grouped in three main categories, which are pictorially represented in Fig.3.1 and discussed as follows:

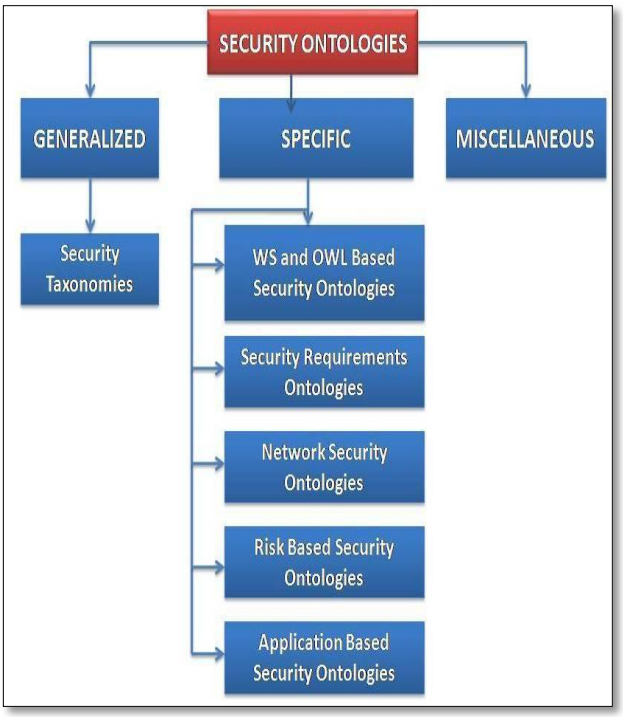

Fig. 3.1: Classification of Security Ontologies

A. ***Generalized Security Ontologies –***

Generalized security ontologies aim and wrapper all security aspects as well as creates explicit terminology of the domain that agree with diverse stakeholders to develop and contribute to a general perceptive of knowledge, which can be logical and analyzed without human intervention. Some of the notable findings have been given as follows:

a) ***Ontology-based Security*** –
A security management structure was built on an arbitrary information system (IS) upon security ontology and knowledge-based resources, which provided reasoning exploiting security knowledge from diverse sources and reusable security knowledge interoperability and aggregation [16].

b) ***Ontology-based Multi-agent Model based on Information Security System*** – The purpose of identifying, extracting and analyzing the main proposals for security ontologies was explained by a formal framework stating the early stage of development and the need of additional research efforts . Based on the established ontology of the information security system domain, a multi-agent model was proposed [17].

c) ***Cloud Computing security taxonomies*** – The preceding study analyzed the security problems unearthed in Cloud Computing based on state-of-the-art Cloud Computing security taxonomies under technological and process-related aspects [18].

B. ***Specific Security Ontologies –***

In the subject of specialized security ontology, some ontologies were proposed in different computational models, which derived a common vocabulary for describing facts related to web services, network, risk, security requirements and application based security etc. Five specific domains of security ontologies that describe specified aspects of security in this category, are given as follows:

1) ***Web Services (WS) and Web Ontology Language (OWL) based Security Ontologies*** – The knowledge representation languages or ontology languages are considered in a family, which are characterized by semantic web such as OWL endorsed by the W3C (World Wide Web Consortium) through Recourses Description Framework (RDF) [20]. Some of the Ontologies are mentioned below:

a) ***OWL-based ontology –*** It provides an extensible ontology for the information security domain, which encompassed the common concepts and precise vocabulary of the domain. The subsequent top-level concepts dealing with assets, threats, vulnerabilities and countermeasures were taken in account while building the ontology [21].

b) ***Ontological structure for information security domain knowledge –*** Research study moved towards the non-core concept having a larger part of the formalizing information security knowledge domain. The study located the exposed threats, which gave rise to follow-up threats that were a latent danger to organizational assets. It also explained the effects of threats on specific security attributes (confidentiality, integrity, availability) which may cause damage to certain assets [22].

c) ***Security Attack Ontology –*** A set of information, which can be reasoned and analyzed automatically was developed through the security attack ontology for web service security threats, which insisted upon an analysis and systematic classification for the development of improved distributed defensive mechanisms using Firewalls and Intrusion Detection Systems (F/IDS) [23].

d) ***OWL-DL Ontology –*** Another research study proposed the defining of a set of rules, which automatically generated semantic relations existing between the provider and requestor security requirements. The transformation of WS-SP (Web Security-Security Policy) into OWL-DL ontology resulted in a semantic approach for specifying web service security policies [24].

e) ***Modeling Enterprise Level Security Ontology –*** Knowledge of the threat and corresponding countermeasures had been integrated into the Modeling Enterprise Level Security ontology, which guaranteed a shared and accurate terminology using OWL and RDF (Resource Description Framework) to represent costs benefit analysis of security mechanisms [25].

2) ***Network Security Ontologies*** - An imperfection in networks and applications are becoming gradually more important, and the distribution of errors and attacks defined may not be stationary. The prior research study on network security services has reviewed threats, vulnerabilities and failure modes, based on standard texts, using well-known concepts, categorizations, and methods, e.g. risk analysis through the medium of asset-based threat profiles and vulnerability attributes. These were used to develop a framework which defined an extensible ontology for network security attacks [26]. A few of the significant

findings of the network security ontologies have been given as follows:

a) ***Security Taxonomy of Internet Security*** – These are taxonomies which clarify several countermeasures of attacks and threats as a general identification of attacks and relationship with the class of categories, through the approach of taxonomies to build strong security system [27].

b) ***Ontology based Model for Security Assessment*** – Research studies described the act of using an ontology for the evaluation of security in network and computer attacks. The study used the method when it was under attack for evaluating the effect of the attack on the system [28].

c) ***Ontology-based Unified Problem Solving Method Development Language (UPML) –*** Researches recommended an ontology structure composed of three parts: Domain ontology, Task ontology, and Resolution ontology based on data found about security risk reduction for the purpose of expanding the knowhow of the concepts of intrusion detection, network safety techniques, security policies, which needed to be processed, stored and shared between experts [29].

d) ***Security Toolbox: Attacks & Countermeasures (STAC) Ontology –*** It was reused in numerous security domains of web applications, network management or communication networks (sensor, cellular and wireless) [30].

e) ***Network Attack Ontology*** – Prior methodology was used to classify computer-based attacks through network attack ontology. The ontology developed an "Attack Scenario" class, inherited from other classes, which characterized and classified computer network attacks. High profile computer network attacks such as Stuxnet and the Estonia attacks were classified through the "Attack Scenario" class [31].

f) ***Ontology-based Attack Model*** – They had proposed a taxonomy, which consisted of five dimensions integrated with attack vector, attack impact, vulnerability, attack target and defense, which incorporated Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE), and Common Platform Enumeration (CPE) from National Vulnerability Database (NVD) [54].

3) ***Security Requirements related Ontologies***

The earlier studies shows that each dedicated model, security requirements for information systems had to be specified while using a number of different levels of abstraction, which necessarily guarantee the correctness of every model [32]. Some security ontologies in order to cope with the definition of security requirements are given as follows:

a) **Ontologies for Security Requirements** – Research studies showed that it is difficult for security experts to communicate clearly about security incidents, so the solution was developed through ontology for Information Systems security that included the concepts and the relations [33].

b) ***Extended Ontology for Security Requirements –*** Researches amalgamate and extend the security ontologies, which include comparative study of primitive concepts in Problem Frames and SecureTropos. The case studies also revealed a number of security requirements adopted with respective representation in terms of the proposed ontology. [34].

c) ***Modelling Reusable Security Requirements based Ontology*** – Risk analysis ontology and requirements ontology were merged to develop, to reuse security requirements and improve security by spotting incompleteness and inconsistency, which elaborated a "lightweight" method in achieving semantic processing in requirements analysis, which specified security requirements, based on security standards [35].

d) ***Security based Ontology for Adaptive Mapping of Security Standards*** – A new security ontology was developed based on improved branching and properties intensity for ontology visualization purposes of security based standards (PCI DSS, ISSA 5173, ISO 27001 and NISTIR 7621) compared to the existing ontologies. The data mapping with ontology resulted in adaptive mapping of any set of security standards that had optimized usage of multiple security standards [36].

e) ***Security and Domain Ontologies for Security Requirements Analysis*** – The research study brought out a method a collection of heuristic production rules which exploited security ontologies and domain ontologies dynamically. The study proved that combining both ontologies is more effective to guide Security Requirements elicitation [37].

f) ***Ontology based Information Security Requirements Engineering*** – In one of the previous research studies, a framework was developed related to information security requirements (ISRs) through ontologies, which used three kinds of generic ontologies (application domain ontology, software requirement ontology and information security ontology that facilitated a

semantic-based interpretation. So engineers have improved our ability to create, manage, and maintain information security requirements. [38].

4) ***Risk-based Security Ontologies***

Some of the security researchers adopt an appropriate set of existing tools and techniques which starts a risk analysis, which increases the adaptation to security solutions leading to more of security solutions to valuable security plan. Some of the related findings are given as follows:

a) ***Security Ontologies: Improving Quantitative Risk Analysis*** – Researchers suggested an ontology, which provided a solid base for an applicable and holistic IT-security approach for small and medium sized enterprises SMEs that enabled low-cost risk management and threat analysis, which was based on the taxonomy of computer security and dependability. Thus, each threat was simulated with a different protection profile with the cost/benefit ratio of individual safeguards [39].

b) **SemanticLIFE** – Researchers explained the fundamental issue for decision makers for organizational security through ontology-based risk assessment method using SemanticLIFE tool which had the ability to use and process local data, resources, which deal with personal information with a paradigm that managed the security and privacy issues of information being processed and shared. [40].

c) **Ontology for Industrial Risk Analysis** – Prior project associated with the developed ontologies, which helped experts to realize the risk analysis studies, aimed to develop an industrial risk analysis support system, which consisted of three main phases: A knowledge base of industrial safety; Index safety-related resources, Case-based reasoning (CBR) system [41].

5) ***Application based Security Ontologies***

These ontologies involved the practical application of ontological resources to specific domains, such as biomedicine or geography. Much work in applied ontology was conceded out within the structure of the semantic web. Some given trend-setting contributions are given as follows:

a) ***Security Ontology to Context-Aware Alert Analysis*** – The research focused on context-aware alert analysis, using OWL and SWRL (Semantic Web Rule Language) and OWL-S based on CIM (Common Information Model), which described context information and security knowledge through ontology. It improved existing alert analysis techniques and provided formal representations, which had been a significant stage for execution of network security management [42].

b) ***Security Ontology for Mobile Applications*** – In this ontology, representation and instantiation were commented; target used was mentioned through integration of the whole approach for security in the mobile world. The research study proposed facts based explanation through the conceptualization of security ontology implemented in OWL-DL semantic language with Protege 4 tool. [43].

c) ***Security Ontology for Mobile Agents Protection*** – Mobile agents had estimated the trust of environment where they will be executed. This issue is addressed in a paper by the use of security ontology. The development of this ontology followed a process, which consists on a set of phases in order to lead to a typical ontology [44].

d) ***NRL(Naval Research Laboratory) Security Ontology*** – It complemented existing ontologies in other domains, which focused on annotation of functional aspects of resources was comprehensive, better organized and capable of representing different types of security statements and class hierarchy. Service Oriented Architecture annotated security aspects of Web service descriptions and queries through NRL Security ontology [45].

e) ***Ontology based on e-health applications*** – The use of security ontology, a set of security patterns were developed based on the knowledge-based approach for the security analysis and design of e-health applications, which identified security and privacy as well as described the validation and compared the approach employed to other methods in the security domain. [47]

f) **Ontology Based Interoperation Service (OBIS)** – Researchers proposed an interoperability solution/tool for the management of a policy decision engine at the stage of the authorization layer of a service oriented system. The method validated in an e-Health scenario for the access of data for diabetes patient disease monitoring management [48].

6) ***Miscellaneous Security Ontologies***

In addition to the aforementioned categories, there appear numerous ontologies, which cannot be placed in any of the categories; therefore such types of ontologies are collected in this miscellaneous category. These have been given as follows:

a) ***SMO***- An object-oriented ontology known as Specification Means Ontology (SMO) was proposed for defining and solving the issues related to security.

SMO helped to choose the precise requirements for a given improvement stage, allowed to track mappings, e.g. solutions were given to cover problems so that it support the project validation process. [49]

b) ***ISMO*** - Information Security Measuring Ontology (ISMO) combined existing measuring and security ontologies and provided security procedures for software developers and malleable applications. ISMO also provided an application with security measuring capability. The Information Security Measuring Ontology illustrated the run-time utilization of the ontology and proved when implementing security measures for applications, was able to recover measures from the ontology at run-time [50].

c) ***SAVO*** - Security Asset-Vulnerability Ontology illustrated that vulnerabilities were exploited by intruders to attacks against peers or systems assets using the quantitative and qualitative analysis which were protected by defensive components. SAVO had combined high-level security policies with concepts, mechanisms and including various ontologies as follows [51]:

- ***SAO*** - Security Attack Ontology was utilized by a coalition of various defensive components (e.g. intrusion detection components) which interacted with each other and shared knowledge about attacks and defenses to ensure better protection.
- ***SDO*** - Security Defence Ontology was mainly used for specification of a number of defensive mechanisms to resist certain security attacks and defined dependences between the security algorithms and standards.
- ***SASO*** - Security Algorithm-Standard Ontology were signed and time-stamped in order to provided integrity, authentication, and non-repudiation using RSA and SHA-256 from new versions of securities.
- ***SFO*** - Security Function Ontology had defined information security issues and assisted developers to create better and more efficient protection against system attacks and failures.

d) ***Vulnerability-Centric Modeling Ontology*** − Vulnerabilities are weaknesses, which assaulters exploit to compromise the system in the requirements, design and the implementation phase. The study intended to amalgamate empirical knowledge of vulnerabilities within the system development process [52].

e) ***Cyber Ontology*** − The potential ontologies and standards utilized to extend the Cyber ontology, which included malware standards, schemas, and terminologies. The Cyber ontology focused on malware and some preliminary aspects of the 'diamond model', which included actors, victims, infrastructure, and capabilities [53].

f) ***Utility Ontologies*** − The research study focused on time, geospatial, person, events, and network operations under super-domain or even mid-level, which would consider for inclusion in the Cyber ontology. [53].

g) ***Security Toolbox: Attacks & Countermeasures (STAC) Ontology*** − was proposed as a semantic-based application to specify the relationships between the main security concepts (cryptographic concepts, security protocols, and security tools) and classifies threats and countermeasures by domain according to the OSI model [55].

h) ***Ontological approach toward cyber security in Cloud Computing*** – Researchers provided an ontology for cyber security operational information based on actual cyber security operations and identified data-asset decoupling data provenance and resource dependency information in cloud computing[56].

i) ***Ontology in Cloud Computing***– The research study discusses on the security issue in clouds, which needs risk assessment, data integrity, recovery, and privacy, regulatory compliance, and auditing. The Design of Security System categorizes two different types of access control mechanisms namely, User Based Access Control (UBAC), and Role Based Access Control (RBAC) [57].

j) ***Ontology-based access control model: cloud security policy*** –Researchers studied on ontology-based access control model, which explained the difference between service providers and users in the permitted access control. Research study helped in context-aware access for proactively applying the access intensity of resource access based on ontology [58].

k) ***Cloud Ontology*** –The study depicted that Cloud Computing has no specialized search engine to match with the user's requirements where ontology acts as imperative responsibility in the cloud computing technology by consolidating analysis of computing resources current across disparate Clouds. Research also provided in depth study about security issues in cloud computing and security measure, which enhance the private and public cloud security levels. [19].

l) ***Security Ontology Driven Multi Agent System Architecture: Cloud Data Storage*** − An ontology based semantically structured, security approached had been adopted by Cloud Computing security domains. It moved towards OWL-based security ontology of Cloud Data Storage (CDS) security and Multi-Agent System (MAS)

Architecture based on ontology had three foremost steps: domain, purpose and scope setting; classes and class hierarchy conceptualization; instances creation. [46]

IV. ANALYSIS AND DISCUSSION

An overview of the related work in the area of security ontology results in a vital topic due to continuous increase in threats, attacks and vulnerabilities in any technology. Presented findings come from generalized ontologies, specific ontologies and miscellaneous ontologies surveys. The restudying of security ontologies will open new devotion for the researchers. A critical analysis of the reported researcher's findings provides following significant conclusions (shown in Fig. 4.1):

- To be at par with emerging technologies, cloud needs to have ontological approach towards cloud security.
- Cloud threats at various stages of cloud implementation need to be defined in form of terminology under the security objectives where threats can be covered.
- There is a need to develop ontology for security concerns in each primary service models Software as a Service, Platform as a Service, and Infrastructure as a Service of the development process of a cloud-based system.
- A complete set of security objectives viz. availability, confidentiality, integrity including others (non-repudiation, trust, governance, legal issue and compliance, privacy, audit, architecture, identity management, access control, software isolation, incident response and application security) needs to be gathered in a framework to implement cloud security countermeasures through the help of ontology.
- Identification of attacks and their relationship within the class of categories, through the approach of taxonomies need to be build on cloud security system.
- An analysis and systematic classification of Cloud security ontology based on threats, attacks, exploited assets, in built vulnerabilities and countermeasures is highly required.
- Accurate terminologies for costs benefit analysis of security mechanisms in Cloud Computing and each cloud threat need to be defined with a different protection profile under its terminology.
- Characterization and classification of attacks can be made a part of cloud in form of classes, which are inherited from generalized security attacks classes.
- Development of cloud security requirements ontology to improve security by detecting incomplete and inconsistent knowledge is highly essential, which will help in achieving semantic processing in requirements analysis.

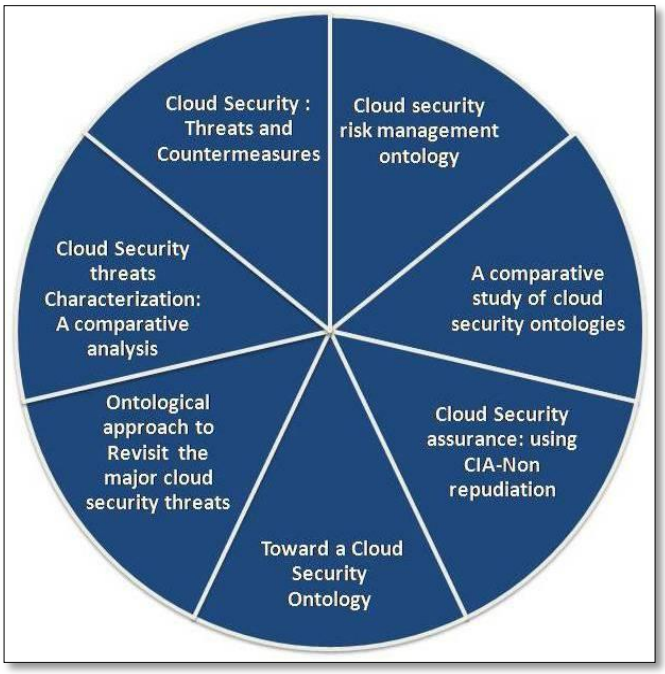

Fig. 4.1: Conclusive Study

V. CONCLUSION AND FUTURE WORK

In any scientific community, defining ontology is considered a difficult and yet, significant task. In this paper, a critical study of security ontologies has been presented in which these ontologies have been grouped into three major categories: Generalized, Specific with sub categories: Web Services (WS) and Web Ontology Language (OWL) based Security Ontologies, Network Security Ontologies, Security Requirements Ontologies, Risk based Security Ontologies and Application based Security Ontologies ; and Miscellaneous. The study of these existing security ontologies has tried to analyze, „how each characteristic of security objectives, assets, vulnerabilities, threats, countermeasures are covered within the aspects of security ontology". In addition, the research has proven whether the proposed security ontologies can be used for defining the cloud security ontology through the conclusive results.

In cloud security ontology, security objectives and requirements must be embedded in the service and deployment models. Major security requirements traceable in the prior studies are basically Confidentiality, Integrity, Governance, Trust, Legal and compliance, etc. [59]. To extend security requirements series one step further, the future work may focus on one or more prominent security requirements such as Non-Repudiation [59], which may enhance the security of the cloud services. A comparative study of cloud security ontology may also be conducted as one of the future

projects to be looked to. And finally, another future study may be conducted to develop ontology for identifying, extracting and analyzing risk, threats, vulnerability along with their countermeasures and their relationships that are managed by every security model through ontology especially in the Cloud Computing architecture.

References

[1]. Margaret Rouse, "Private paas offerings: benefits. Challenges. Best practices and more", Essential Guide. Published: 21 Dec 2010.

[2]. "Cloud Computing", http://en.wikipedia.org/wiki/Cloud_computing [Accessed: 11-02-2014].

[3]. Banerjee, S. K. Pandey, "Software Security Rules, SDLC Perspective", International Journal of Computer Science and Information Security, IJCSIS, Vol. 6, No. 1, pp. 123-128, October 2009, USA.

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

[5]. Mustafa K., Rehman S., Pandey S. K. (2009, March): "Confidentiality related security assessments", IEEE International Advance Computing Conference, Patiala.

[6]. Pandey S. K. & Mustafa K. (2010, July-Aug), "Security Assurance: An Authentication Initiative by Checklist", International Journal of Advanced Research in Computer Science, 1(2), 110-113.

[7]. 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.

[8]. LI Shan-Ping, YIN Qi-Wei, HU Yu-Jie, GUO Ming, FU Xiang-Jun, "Overview of Researches on Ontology", Journal of Computer Research and Development, 2004-07.

[9]. Anoop Singhal and Duminda Wijesekera. "Ontologies for Modeling Enterprise Level Security Metrics", Proceeding of the sixth annual workshop on CSIIRW ¨10. ACM Article No. 58.

[10]. Stefan Fenz. "Security Ontology" http://stefan.fenz.at/research/security-ontology/ [Accessed: 03-01-2014].

[11]. S. K. Pandey, K. Mustafa, "Access Control and Rights related Risk Assessment" , International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 1, Jan-Feb 2012, pp.1174-1178 .

[12]. 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.

[13]. 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.

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

[15]. Pachipala Yellamma, N arasimham Challa and V Sreenivas, "Intelligent Data Security in Cloud Computing", International Journal of Current Engineering and Technology, Feb 2014, Vol.4, No.1.

[16]. Tsoumas. B. andGritzalis. D. "Towards an Ontology-based Security Management", AINA 2TH International Conference Advanced Information Networking Applications.,2006 , Vol.1 .pp.985-992

[17]. I. Gorodetski. L. J. Popyack. I. V. Kotenko. V. A. Skormin. "Ontology-Based Multi-agent Model of an Information Security System". 7th International Workshop. RSFDGrC¨99. Nov 9-11.1999, Proceedings, pp.528-532.

[18]. Madhan Kumar Srinivasan, K. Sarukesi, Paul Rodrigues, M.SaiManoj, P.Revathy, "State-of-the-art Cloud Computing security taxonomies: a classification of security challenges in the present Cloud Computing environment", http://dl.acm.org/citation.cfm?id=2345474 [Accessed: 11-02-2014].

[19]. 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.

[20]. Web Ontology Language, http://en.wikipedia.org/wiki/Web_Ontology_ Language #Semantic_web_standards [Accessed: 12-02-2014].

[21]. Herzog Almut. ShahmehriNahid and Duma Clauda. "An Ontology of Information Security". International Journal of Information Security and Privacy. 2007, Vol. 1 .Issue 4. pp.23 .

[22]. Fenz S. Ekelhart A., "Formalizing information security knowledge". In 4th International Symposium on Information. Computer. And Communications Security (ASIACCS ¨09), pp. 183-194, (2009).

[23]. Vorobiev. A. and Jun Han. "Security Attack Ontology for Web Services". Second International Conference on Semantics. Knowledge and Grid. 2006. pp.42.

[24]. Denker. G. L. Kagal, T. Finin.: "Security in the Semantic Web using OWL". Information Security Technical Report. 10(1): p. 51-58. . (2005).

[25]. Stefan Fenz. "Ontology-based Generation of IT-Security Metrics". SAC ¨10 Proceeding of the 2010 ACM Symposium on Applied Computing. pp. 1833-1839.

[26]. Andrew Simmonds, Peter Sandilands, Louis van Ekert "An Ontology for Network Security Attacks" Applied ComputingLecture Notes in Computer Science Volume 3285, 2004, pp 317-323.

[27]. Ali Abbas, Abdulmotaleb El Saddik, and Ali Miri , "A State of the Art Security Taxonomy of Internet Security: Threats and Countermeasures", GESTS Int"l Trans. Computer Science and Engr., Vol.19, No.1.

[28]. Jian-boGao, Bao-wen Zhang ,Xiao-hua Chen, ZhengLuo, "Ontology-based model of network and computer attacks for security assessment" Journal of Shanghai Jiaotong University (Science) Volume 18, Issue 5, pp 554-562.

[29]. Fong-Hao Liu, Wei-Tsong Lee "Constructing Enterprise Information Network Security Risk Management Mechanism by Ontology" , Tamkang Journal of Science and Engineering, Vol. 13, No. 1, pp. 7987 (2010) .

[30]. Amelie Gyrard, Christian Bonnet, KarimaBoudaoud, "The STAC (Security Toolbox: Attacks & Countermeasures) ontology" ACM Companion, May 13–17, 2013 .

[31]. RP van Heerden, B Irwin, ID Burke "Classifying Network Attack Scenarios using an Ontology" http://eprints.ru.ac.za/4170/1/Classifying%20Network.pdf

[32]. "Security Ontology Definition", Policy and Security Configuration Management, PoSecCo, 01.10.2010, http://www.posecco.eu/fileadmin/POSECCO/user_upload/deliverables/ 3.2_SecurityOntologyDefinition.pdf [Accessed: 13-02-2014].

[33]. Souag Amin,.Salinesi Camille, Comyn-Wattiau. Isabelle, "Ontologies for Security Requirements: A Literature Survey and Classification". Proceedings CAiSE 2012 Intenat ional Workshop. 25-26 June 2012, Vol. 2012, pp .61-69.

[34]. Fabio Massacci, , John Mylopoulos, Federica Paci, TheinThunTun, Yijun Yu, "An Extended Ontology for Security Requirements", http://securitylab.disi.unitn.it/lib/exe/fetch.php?media=wisse-cameraready-paper7.pdf [Accessed: 14-02-2014].

[35]. JoaquínLasheras, Rafael Valencia-García, JesualdoTomásFernández-Breis and AmbrosioToval, "Modelling Reusable Security Requirements based on an Ontology Framework" http://ws.acs.org.au/jrpit/JRPITVolumes/JRPIT41/JRPIT41.2.119.pdf [Accessed: 15-02-2014].

[36]. SimonaRamanauskaite, DmitrijOlifer, NikolajGoranin, NikolajGoranin, AntanasČenys, AntanasČenys, "Security Ontology for Adaptive Mapping of Security Standards", International Journal of Computers, Communications & Control (IJCCC) , Vol 8, No 6 (2013) .

[37]. Souag, A., Salinesi, C. ; Wattiau, I. ; Mouratidis, H., "Using Security and Domain Ontologies for Security Requirements Analysis" , Computer Software and Applications Conference Workshops (COMPSACW), 2013 IEEE 37th Annual , 22-26 July 2013, pp. 101 – 107 .

[38]. AzeddineChikh, Muhammad Abulaish, Syed IrfanNabi, KhaledAlghathbar, "An Ontology Based Information Security Requirements Engineering Framework" http://www.abulaish.com/uploads/STA11B.pdf [Accessed: 16-02-2014].

[39]. Ekelhart, A., Fenz, S., Neubauer, T. "Security Ontologies: Improving Quantitative Risk Analysis" 40th Annual Hawaii International Conference on System Sciences, HICSS 2007 pp. 156a.

[40]. Mansoor Ahmed, Amin Anjomshoaa, ThoManh Nguyen, and A Min Tjoa, "Towards an Ontology-based Organizational Risk Assessment in Collaborative Environments Using the SemanticLIFE" http://publik.tuwien.ac.at/files/pub-inf_4730.pdf [Accessed: 17-02-2014].

[41]. AbouAssali A., Lenne D., Debray B.: "Ontology development for industrial risk analysis". In: IEEE International Conference on Information & Communication Technologies: from Theory to applications (ICTTA 2008), Damascus, Syria (April 2008).

[42]. HuiXu, Debao Xiao, Zheng Wu, "Application of Security Ontology to Context-Aware Alert Analysis" ICIS 2009. Eighth IEEE/ACIS International Conference on Computer and Information Science, 1-3 June 2009, pp.171 – 176.

[43]. Beji, S, El Kadhi, N., "Security Ontology Proposal for Mobile Applications, MDM '09, Tenth International Conference on Mobile Data Management: Systems", Services and Middleware, 18-20 May 2009, pp. 580 - 587 .

[44]. S. Hacini and R. Lekhchine, "Security Ontology for Mobile Agents Protection, International Journal of Computer Theory and Engineering", Vol. 4, No. 3, June 2012

[45]. Anya Kim , Jim Luo , Myong Kang ,"Security Ontology for Annotating Resources", Research Lab, NRL Memorandum Report

[46]. Amir Mohamed Talib, RodziahAtan, Rusli Abdullah and MasrahAzrafiAzmiMurad "Security Ontology Driven Multi Agent System Architecture for Cloud Data Storage Security Ontology Development", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.5, May 2012 .

[47]. S. Dritsas, L. Gymnopoulos, M. Karyda, T. Balopoulos, S. Kokolakis, C.Lambrinoudakis and S. Katsikas, "A knowledge-based approach to security requirements for e-health applications" http://www.ejeta.org/specialOct06-issue/ejeta-special-06oct-4.pdf [Accessed: 18-02-2014].

[48]. Ioana Ciuciu, Brecht Clear hout, Louis Schilders, and Robert Meersman "Ontology-Based Matching of Security Attributes for Personal Data Access in e-Health" , OTM 2011, Part II, LNCS 7045, pp. 605–616, 2011 Springer-Verlag Berlin Heidelberg.

[49]. Andrzej Bialas "Ontology-based Security Problem Definition and Solution for the Common Criteria Compliant Development Process", 2009 Fourth International Conference on Dependability of Computer Systems IEEE Computer Society.
[50]. AnttiEvesti, Reijo Savola, Eila Ovaska, Jarkko Kuusijärvi "The Design, Instantiation, and Usage of Information Security Measuring Ontology" 01/2011
[51]. Artem Vorobiev, Jun Han, and Nargiza Bekmamedova"An Ontology Framework for Managing Security Attacks and Defences in Component Based Software Systems" 19th Australian Conference on Software Engineering IEEE Computer Society 2008.
[52]. GolnazElahi, Eric Yu, Nicola Zannone, "A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations?" 28th International Conference on Conceptual Modeling, November 9-12, 2009 Proceedings. Springer Berlin Heidelberg, Vol. 5829 pp 99-114 .
[53]. Leo Obrsta, Penny Chaseb, Richard Markeloffa, "An Ontology of the Cyber Security Domain", http://ceur-ws.org/Vol-966/STIDS2012_T06_ObrstEtAl_CyberOntology.pdf [Accessed: 19-02-2014].
[54]. Jian-boGao, Bao-wen Zhang ,Xiao-hua Chen, ZhengLuo, "Ontology-based model of network and computer attacks for security assessment" Journal of Shanghai Jiaotong University (Science) Volume 18, Issue 5 , pp 554-562.
[55]. AmelieGyrard, Christian Bonnet, KarimaBoudaoud, "The STAC (Security Toolbox: Attacks & Countermeasures) ontology" ACM Companion, May 13–17, 2013.
[56]. Takeshi Takahashi, 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.
[57]. Keerthana Subramani, Priya Dharshini Ponniah Rajagopal, Savitha Sundaramoorthi, "Ontology in Cloud Computing", http://cloudontology.wikispaces.asu.edu/Use+of+Ontology+in+Cloud+C omputing#Use Of Ontology In Cloud Computing-Design of Security System [Accessed: 19-02-2014].
[58]. Chang Choi, Junho Choi, Pankoo Kim , "Ontology-based access control model for security policy reasoning in cloud computing", The Journal of Supercomputing, Volume 67, Issue 3 , pp 711-722.
[59]. S. K. Pandey, K. Mustafa, "Non-Repudiation Related Risk Assessments" International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 2, August 2012.

AUTHORS

Ms. Vaishali Singh is presently working as an Research Scholar in the Department of Computer Science, Jagannath University, 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 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 expert.