Institute of Advanced Engineering and Science

International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.1, No.4, October 2012, pp. 210~218
ISSN: 2089-3337

Towards Information Security Metrics Framework for Cloud Computing

Muhammad Imran Tariq*
* Departement of Computer Science and Informatin Technology, University of Lahore, Pakistan

Article Info

Article history:

Received Sept 05th, 2012
Accepted Sept 26th, 2012

Keyword:

Cloud Computing
Security issues
Security metrics framework
Information Security metrics

ABSTRACT

Cloud computing has recently emerged as new computing paradigm which basically aims to provide customized, reliable, dynamic services over the internet. Cost and security are influential issues to deploy cloud computing in large enterprise. Privacy and security are very important issues in terms of user trust and legal compliance. Information Security (IS) metrics are best tool used to measure the efficiency, performance, effectiveness and impact of the security constraints. It is very hard issue to get maximum benefits from Information security metrics in cloud computing. The aim of this paper is to discuss security issues of cloud computing, and propose basic building blocks of information security metrics framework for cloud computing. This framework helps cloud users to create information security metrics, analyze cloud threats, processing on cloud threats to mitigate them and threat assessment.

Corresponding Author:

Muhammad Imran Tariq,
Departement Computer Science and Information Technology,
The University of Lahore,
1-KM Raiwind Road, Lahore, Pakistan.
Email: imrantariqbutt@yahoo.com

1. INTRODUCTION

Cloud computing is becoming more attractive as it provides all computing services on your desktop or somewhere inside your company's network. Cloud computing services are provided by the another company and can be acceessed over the intenet. Cloud users can use these services without knowing how these resources are being managed and thier location.

Cloud computing has several constratints which are bareer in cloud deployment. The major constraint is security. Till todate, lot of efforts has been made to improve security in cloud computing but still cloud computing (especially public cloud) is insecure. İnformation security threats often influence to the corporate processes and operations directly.

To handle these challenges, different information security frameworks, Information security standards and guides are exited and it is very hard and careful process to select one of the best framework and standard based on their security requirements.

Information security metrics is best tool to measure the security of the cloud service provider e.g. how secure is cloud service provider or is it deployed comprehensive security measure?

Cloud security threats can be drived from metrics and solve through threat modeling techniques. Mostly, these techniques are particularly for networks but not specific for cloud computing.

This paper is organized into 04 sections. The first section is about cloud computing definations, brief about information security and metrics. The following section will discuss cloud security issues. Then the section three will present state of the art related with security metrics and threat modeling and the next section will propose basic building block of information security metrics framework for cloud computing. The last section is about conclusion and future work.

2. CLOUD SECURITY ISSUES

Cloud computing has several advantages over traditional computing which makes it better and powerful solution for cloud users. In public and private cloud, senstitive data and critical appliations are shared in cloud environment. Several security concerns are arises that need to be addressed.

This section describes about cloud security issues, and cloud security threats when considering cloud computing. Some of the cloud computing issues faced by the cloud customers:

- **Data location**
- **Data theft**
- **Data loss**
- **Data integrity**
- **Privacy ıssues**
- **Regulatory requirements**
- **Diaster revovery / Business continuity plan**

2.1. Data location

Cloud networks span over continents, countries and regions, the physical location of the data are spread accross several geographical areas. The cloud user has no physical access over the data even does not know about its location. The cloud service provider (CSP) also does not reveal where all data are stored. Some time, the CSP store one customer data on differenct locations or countries [11]. Therefore, different country privacy laws are applied one one customer data. The cloud user should require from CSP to store and process data in a specific jourdictions and strictly obey privacy rules of those juridications [1],[2].

2.2. Data theft

Most of cloud service providers offer the services which they are lease from other service provider (external). The cloud users does not know that's going behind the scene and they are just supposing that it is their service provider's service [2]. There is a high possibility that the external service provider attacked by malicious users and customer data may stolen.

2.3. Data loss

It is very serious and dangerous problem in cloud computing. If the vender shutdown its business due to some legal obligations or some sort of financial problems then cloud user data will be loss or might be misuse [1],[3].

2.4. Data integrity

In cloud computing, anyone from any location can access the data. Cloud does not differentiate between common data and sensitive data [6]. It is necessary for the CSP to ensure the integrity by making their system capable to check over the cloud data from any illegal modification [10]. To overcome data integrity security issue, Third party auditor assistance must be use [13].

2.5. Privacy issues

The cloud users store their sensitive data on CSP site and its vender's responsibility to secure information from other operators and intruders. The CSP should implement multiple level password and code words protection to grant access on sensitive data and implement current privacy laws [4]. The cloud user should to thoroughly read privacy issues before using cloud computing [5].

2.6. Regularity requirments

The Cloud venders often claim that they have implemented all security measures but in reality it is not [8]. The cloud user does not know about the exact security measures taken by the CSP. Many organizations in USA, Canada, or the European Union have implemented regulatory requirements (e.g. ISO/IEC 27002, ITIL and COBIT). The cloud user must ensure that his / her CSP meet these requirements [2], [7].

2.7. Diaster recovery

As mentioned above, the cloud user does not know about the data physical locations. Their all respective physical locations face natural and unnatural disaster threats like fire, storm, flood, earth kicks and loss of electric power [9]. To mitigate these issues, backup / copies of data on multiple countries is recommended [2].

2.8. Cloud Security threats

Cloud computing faces same security threats that are currently found in the existing networks (LAN, WAN, Intranet). These threats and risks came in cloud computing in various forms. Some of the network issues occur in cloud computing are listed below [6], [8].

- Denial of Service
- Man in the Middle
- Net Sniffing
- Port Scanning
- SQL Injection Attack
- Flooding attack

Cloud Security Alliance (CSA) in 2010 did a research on cloud computing threats and identified top 10 cloud threats [12] in which 05 major 05 threats are given below:

- Unknown Risk Profile
- Shared Technology Vulnerabilities
- Malicious Insider
- Abuse and Nefarious Use of Cloud Computing
- Account. Service & Traffic Hijacking

Moreover, the cloud faces XML Signature Element Wrapping, browser security and Cloud Malware Injection Attack threats [6].

3. STATE OF THE ART

In cloud computing, information security metrics provide a useful and practical way to measuring information security. Different security metrics were proposed to enhance the security of the organization. Wayne et al. [14] has identified technical security metrics for the operators of control systems. Inigo. G. et al. [15] proposed resource level metrics for specifying fine grain guarantees on CPU performance. Mark. D. [16] discussed the possibility of creating of meaningful security metrics for communication system and proved that it is not possible to measure trust in an absolute sense. Patrick. J. [17] discussed operational level security metrics and described how operational management can take benefits from security metrics.

Moreover, various taxonomies and state of the art for security metrics were written to explore existing security metrics and their merits and demerits. Reijo. S. [18], [19] and [20] surveyed existing security metrics and proposed security metrics taxonomy for ICT product Research and Development (R&D). These taxonomies can be used to enhance the composition of feasible security metrics. Rostyslav. B. et al. [21] examined current state of the art information security measurement and practical issues concerning the subject matter. SANS [22] defined seven key steps which could be use as guide in the process of establishing security metrics program.

The U.S National Institute of Information Standards and Technology (NIST) [23] presented its security metrics taxonomy namely NIST SP 800-26 and NIST SP 800-55. NIST divided security metrics into three categories (management, technical and operational) and seventeen sub-categories.

Vaughn et al. [25] propose taxonomy for information assurance metrics and divided the same into two distinct categories (organizational security metrics and metrics for Technical Target of Assessment). Seddigh et al. [24] introduce information assurance metrics taxonomy for IT Network assessment. This taxonomy has three categories (security, Quality of Service (QoS) and availability) and further considered technical, organization and operational metrics under these three metrics.

Threat Modeling is a technique used to identify, analyse and mitigate threats. Ebenezer. A. et al. [26] proposed a goal oriented approach for Security Threat Modeling and applied approach by Modeling and analysing security threats of an online banking system. SANS [27] defined the processes to create and use threat model and discussed the significance of application security at design time.

Jesus. L. et al. [28] used scenario driven approach to develop common security metrics framework for cloud. This proposed framework takes Risk-driven Security Metrics as input; analyze threats, defined security requirements and policy formalization. Finally the security is evaluated by using quantitative security levels. The author introduces the scenario based common processes to handle cloud security threats. These processes are resembles to security threats modeling processing like Microsoft Security Development Lifecycle (SDL Threat Modeling). The authors used “Risk-Driven Security Metrics” approach as input without its detail about it and used threat analysis phase to identify security risks instead of describing analysis techniques. Authors used ENISA guide as input for next step i.e. Security requirement in his proposed framework. Moreover, the authors do not mentioned the detail of each phase.

4. SECURITY METRICS FRAMEWORK

Many organizations have inadequate or sometimes have no experience to develop information security metrics, identify threats for their process control system. To help them in preparing a suitable set of security metrics, identify threats and mitigation threat, common framework for developing and integrated set of processes control information security metrics and threats is proposed for cloud computing. The proposed information security metrics framework for cloud computing is shown in Figure 1. The information security metrics framework has four major stages:

1. **Metrics Preparation**
2. **Threat Identification and Analysis**
3. **Threat Processing**
4. **Application**

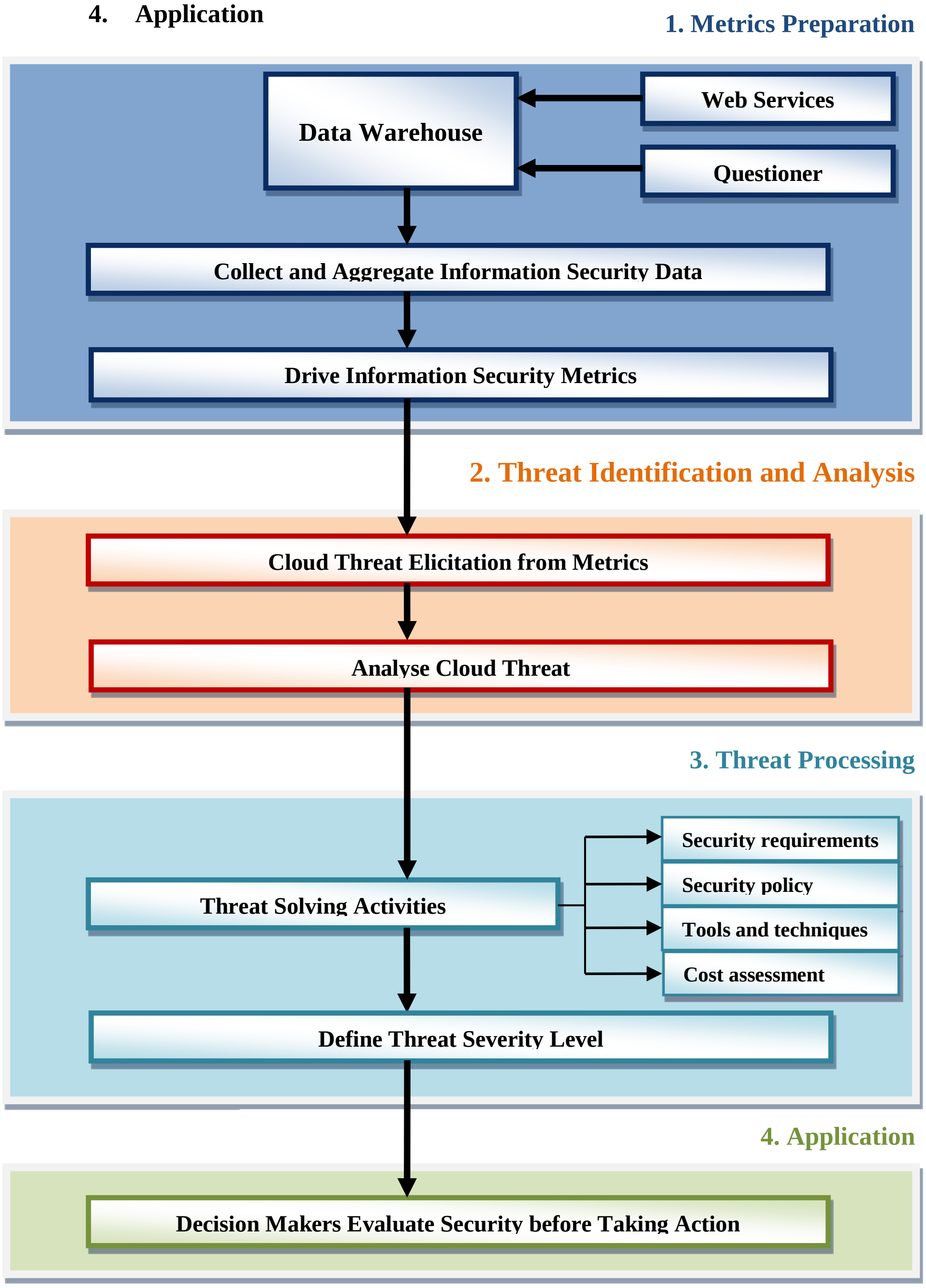
1. Metrics Preparation
Data Warehouse
Web Services
Questioner
Collect and Aggregate Information Security Data
Drive Information Security Metrics
2. Threat Identification and Analysis
Cloud Threat Elicitation from Metrics
Analyse Cloud Threat
3. Threat Processing
Threat Solving Activities
Security requirements
Security policy
Tools and techniques
Cost assessment
Define Threat Severity Level
4. Application
Decision Makers Evaluate Security before Taking Action

Figure 1. Framework for Information Security Metrics for Cloud Computing

4.1 Metrics preparation

The IS metrics preparation phase involves information security metrics development team to develop useful information security metrics. Metrics preparation phase consist of two major steps:

1. Collect and Aggregate Information Security Data
2. Drive Information Security Metrics

4.1.1. Collect and aggregate information security data

This is first step in which data regarding information security will be obtained through different techniques like web services, questioners and data warehouse.

4.1.1.1. Web services

Multiple web services are available that gather information security related information from different sources. The same information can then be made visible to users by using various visualization tools. To make information meaningful, information is linked to Key Performance Indicators (KPIs), IS standards and metrics. [44].

Security Information Management (SIM) also referred as Security Event Management (SEM) tools that report on information security data collected from a number of sources. This data can be normalized, aggregated, correlated and archived from various data stores [44].

4.1.1.2. Questionnaire

Information Security metrics framework uses questionnaire technique to configure desire performance levels of KPIs (minimum level of performance and desired level of performance) and metrics. Questionnaire can be base on SAN'S audit checklist and internal and external audit results [44].

4.1.2. Drive information security metrics

The output of the section 1 is information security related data that abstracted from various sources and stored in data warehouse. KPIs have various metrics associated with it and used to measure the effectiveness of security control. The data warehouse stores metrics information like description, weighting value, desired value, actual value and minimum acceptable value for the metrics [44].

There are internationally accepted frameworks, standards and guides are available for guidance in metrics development. IT Infrastructure Library (ITIL) and Control Objectives for Information and related Technology (CobiT) are renowned frameworks. International Organization for Standardization (ISO) has ISO/IEC 27002 information security and control standards which also can be used to drive information security metrics. At present, ISO/IEC WD 27018 and ISO/IEC WD TS 27017 ISO information security standards are under development. SAN'S has also published information security metrics guide which is very helpful for cloud users to drive information security metrics.

4.2. Threat identification and analysis

The 2nd Phase of this proposed framework is about threat elicitation and analysis. In this phase, the threats are identified from information security metrics and different techniques like threat tree are applied to analyze the threat.

4.2.1 Cloud threat elicitation from metrics

After developing information security metrics, the next step is to elicit cloud security threats from metrics. Different approaches has already been in practice for threat elicitation like STRIDE model and categorized threat list. Furthermore, Myagmar. S. et al. [27] and Ebenezer et al. [26] described methods for threat elicitation.

The STRIDE classified the threats as Spoofing, Tampering, Repudiation, Denial of service, and Elevation of privilege can be used to elicit security threats [26].

Mark. M. et al. [30] presented threat model based on based on threat metrics and discussed various metrics sources.

4.2.2. Analyse cloud threat

This is most critical section of the security metrics framework in which cloud threats are critically analyzed. Threat analysis goals are to discover what, why, when, where, why and how threat attack on the system and what are the security risks of a cloud system. This step is very important for threat solving activities and adequate security mechanism [28]. It is important for threat analyst to understand the threats that exist in the environment.

At present, several threat analysis, assessment and modeling methods are existed to guide users about this section [31].

Threat tree, attack tree and some same type of methodologies are used to identify threat type, represent threat and analyze threat [31]. In tree analysis, top-down approach is used to determine viable threat vectors.

Jones [32] presented threat assessment methodology in which threat agents are identified and categorized to analyze their capabilities. The motivational factors of the agents are also examined. Vulnerability Instantiation Methodology (VIM) is a two-stage method that uses vulnerabilities and their relationships to identify and analyze threats.

Threat assessment models are also used to analyze threats like Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [34] framework was designed to identify and manage security risks. It helps organization to identify information assets, threats to those assets and vulnerabilities that may expose those assets to the threats. Similarly Amenaza IT Threat Tree Modeling System [35] was developed to model threats in hierarchy trees. It calculates risk of the threat and impact of the threat to get risk value.

European Network and Information Security Agency (ENISA) [33] has made assessment of the security risks and benefits of cloud computing. Moreover it provided security guidance for potential and existing users of cloud computing.

4.3. Threat processing

After Analysis of threat, this phase is defined different activities that help cloud users to process on identified IS threats. This phase is very critical & technical and required due concentration of threat solving team.

4.3.1. Threat solving activities

This is very important section of this proposed framework. Threat solving activities are divided into of four (4) sub activities which are as under:

- Security requirements
- Security policy
- Tools and techniques
- Cost assessment

4.3.1.1. Security requirements

Requirement statement is consisting of goals that must be fulfilled in order to mitigate threat [29]. To solve the cloud threat, it is essential to define security requirements. This section identify about the action(s) to be taken in order to minimize the probability of a particular threat or risk [28].

For example, the threat is *"Attacker uses DoS attacks to reduce availability of the system"*. The attack tree that used in previous section analyzed that this threat can be either flooding the network interface or filling up the available disk space [35]. The requirement needs to mitigating said threat could be *"The system shall not allow any user to successfully use DoS attack to reduce availability of the system"* [35].

ENISA [33] made assessment of cloud computing risks and its associated requirements to mitigate cloud threats. Cloud Security Alliance (CSA) [37], [38] white papers (Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 and Cloud Control Matrix) are also very helpful in defining security requirements.

4.3.1.2. Security policy

A security policy is also called as set of security requirements mentioned in previous section. A security policy is defined against each security requirements. For example, the National Institute of Standards and Technology (NIST) provide a guidelines and recommendations to users to securing public Web servers that "*all traffic between the Internet and Web server*" should be controlled and that "*all inbound traffic to the Web server except traffic which is required, such as TCP ports 80 (HTTP) and/or 443 (HTTPS)*" should be denied.

4.3.1.3. Tools and techniques

Analysis of tools and techniques is a process that uses to find out solution of threat. Information for tools and techniques can be obtained from different sources like websites, news feeds, IRC message boards, security forums, groups and intelligent activities [39].

It is fact that all cloud management tools not work equally for all cloud providers and not allows customers to manage their internal and external security as single unit [40].

Examples of Tools are HyTrust's virtual management appliance; it provides server configuration templates, VMWARE vSphere security configuration assessment against industry frameworks. CohesiveFT sells cloud security tools (VPN-Cubed virtual firewall and router), and management tools to build VM templates and monitoring of management tasks [40].

4.3.1.4. Define threat severity level

After analysis of tools and techniques for cloud threats, it is essential to define threats severity levels. The use of severity levels always plays an important by informing the peoples about the event should trigger within time frame. Cloud Security Alliance (CSA) [41] in its white paper (Top threats to cloud computing V1.0) identified top 10 cloud security threats with their impacts and given recommendation against each threat. Symantec.cloud [43] defined four (4) threat levels for cloud.

In general, threat severities levels can be classified into five levels based on their severity [43], [42]. The highest severity level poses the most serious threat to cloud security. The following Table 1 defines five severity levels for cloud security threats.

Severity	Level	Description
1	Minimal	In minimal, the intruder can just get information about the user by performing passive attack like eavesdropping and session hijacking. Continuous monitoring is required.
2	Medium	The hacker or intruder can get sensitive information about the users and there is no discernible network activity.
3	Serious	This level is developed when the intruder may able to get partial access of resources or able to get read access of specific files. Serious level condition is fulfilled when malicious code reaches moderate risk rating.
4	Critical	Critical situation arise when intruder gain control on host or have full access to read the files or malicious code reaches sever risk rating. Increased monitoring is required.
5	Urgent	It is highest severity level in which intruder can easily gain full control on the host. The intruder gain entire network control with read and write access. Top priority should give to urgent level.

Table 1. Defination of severity levels

4. Application

The last activity of this framework focus on the use of the security metrics and threat severity levels by the decision makers. They evaluate the security and take suitable actions. In this last phase, IS metrics, cloud security threats and severity levels are accessed by the decision makers. Risk assessment may be used to provide additional information to support this last activity.

Security assessment is continuous process. Information Security metrics development, threat identification and assessment activities never end. It is recommended that upgrade metrics as time to time new threats and vulnerabilities came

5. COMMENTS AND CONCLUSION

Cloud Computing is itself a virtualization of resources. These resources can be accessed with minimal mangement and without requiremnet of having knowledge of system that deliver it. Cloud has lot of benefits (like scalability, pay as per use, share resource in on place and less management) over traditional computing which makes it famous and powerful.

Cloud Service Providers claims that they meet full security requirements but in reality it is not. To evaluate performance and effectivness of cloud service provider's deployed security as per terms and conditions laid down in Service Level Agreement (SLA), Information Security metrics are best tools. There are several techniques to develop security metrics in which one is used in this paper proposed framework.

Clouds faces various security issues and same kind of threat and vulnerabilities like traditionals networks. To mitigate these threats, attack tree, threat tree and similar tree-based threat modeling methodologies can be used.

The proposed informaton security metrics framework for cloud computing helps the organizations to develop cloud security metrics, identify threats from metrics, analysis and mitigate threat. The proposed framework is flexible, open and technology-agnostic and able to be extended through new addition of new security metrics or as per organizations specific requirements.

As future work, Several research challenges has been identified with the proposed informatoin security metrics framework for cloud computing particularly with the quantititive evaluation of security threats. Moreover, it is also under consideration to make different scenarios that support this proposed framework and develop security evaluation techniques for better decison about security threats.

REFERENCES

1. A. Bisong and M. Rahman, “An overview of The Security Concerns in Enterprise Cloud Computing,” *International Journal of Network Security & Its Applications (IJNSA)*, vol. 3, pp. 30-45, 2011.
2. B. Meena and K. Challa, “Cloud Computing Security Issues with Possible Solutions,” *International Journal of Computer Science and Technology (IJCST)*, vol. 1, pp. 340-344, 2012.
3. M. Al-Mosry, *et al.*, “An Analysis of the cloud computing security problem,” *Applied Security (Appsec) 2010 cloud workshop*. 2010.
4. P. Kumar, *et al.*, “Effective Ways of Secure, Private and Trusted Cloud Computing,” *International Journal of Computer Science Issues (IJCSI)*, vol. 8, pp. 412-421, 2011.
5. K. Chaitanya, *et al.*, “Study of security issues in cloud computing,” *International Journal of Computer Science and Technology (IJCST)*, vol. 2, pp- 51-53, 2011.
6. S. Qaisar and K. F. Khawaja, “Cloud computing: Networks/Security threats and countermeasure,” *Interdisciplinary Journal of Contemporary Research in Busines (IJCRB)*, vol. 3, pp. 1323-1329, 2012.
7. K. Shade, *et al.*, “Cloud Security and Challenges,” *International Journal of Computer Networks (IJCN)*, vol. 3, pp. 247-255, 2011.
8. K. Curran, *et al.*, “Security issues in cloud computing,” *Elixir Journal*, vol. 38, pp. 4069-4072, 2011.
9. D. Jamil and H. Zaki, “Security issues in cloud computing and countermeasures,” *International Journal of Engineering Science and Technology (IJEST)*, vol. 3, pp. 2672-2676, 2011.
10. A. A. Atayero and O. Feyisetan, “Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption,” *Journal of Emerging Trends in Computing and Information Sciences (JETCIS)*, vol. 2, pp. 546-522, 2011.
11. K. Fakushima, *et al.*, “Towards Secure Cloud Computing Architecture- A Solution Based on Software Protection Mechanism,” *Journal of Internet Services and Information Security (JISIS)*, vol. 1, pp. 4-17, 2011.
12. Cloud Security Alliance, “Top threats to cloud computing, version 1.0,” *Cloud Security Alliance, http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf*, 2010.
13. D. Attas and O. Batrafi, “Efficient integrity checking technique for securing client data in cloud computing,” *International Journal of Electrical & Computer Science (IJECS-IJENS)*, vol. 3, pp. 43-48, 2011.
14. W. Boyer and M. Mcqueen, “Ideal Based Cyber Security Technical Metrics for Control Systems,” *2nd International Workshop on Critical Information infrastructure Security*, 2007.
15. I. Goiri, *et al.*, “Resource-Level QoS Metric for CPU-Based Guarantees in Cloud Providers,” *Springer-Verlag Berlin Heidelberg 2010*, pp. 34-47, 2010.
16. J. Rosenblatt, “Security Metrics: A Solution in Search of Problem,” *Education Quarterly*, 2008.
17. J. P. Ravenel, “Effective Operational Security Metrics,” *Information System Security Association (ISSA) Journal*, 2006.
18. R. Savola, “A Novel Security Metrics Taxonomy,” *7th Annual Information Security South Africa (ISSA) conference, Johannesburg, South Africa*, 379-390, 2008.
19. R. Savola, “A Security Metrics Taxonomization Model for Software-Intensive System,” *Journal of Information Processing System*, vol. 5, pp. 197-206, 2009.
20. R. Savola, “Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry,” *International Conference on Software Engineering Advances (ICSEA)*, pp. 60-66, 2007.
21. R. Barabanov, *et al.*, “Information Security Metrics-State of the Art,” *DSV Report series No 11-007*, 2011.
22. S. C. Payne, “A Guide to Security Metrics,” *http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55*, 2006.
23. E. Chew, *et al.*, “Performance Measurement Guide for Information Security,” *NIST Special Publication 800-55 Revision 1*, 2008.
24. N. Seddigh, *et al.*, “Current Trends and Advances in Information Assurance Metrics,” *Proc. of the 2nd Annual Conference on Privacy, Security and Trust (PST 2004), Fredericton, NB*, pp. 197-205, 2004.
25. R. B. Vaughn, *et al.*, “Information Assurance Measures and Metrics: State of Practice and Proposed Taxonomy,” *Proceedings of 36th Hawaii International Conference on System Sciences (HICSS 03)*, 2003.

26. E. A. Oladimeji, *et al*., “Security Threat Modeling and Analysis: A Goal-Oriented Approach,” *Proceedings of the 10th International Conference on Software Engineering and Applications (SEA '06),* pp. 178-185, 2006.
27. SANS, “Threat Modeling: A Process To Ensure Application Security,” *http://www.sans.org/reading_room/whitepapers/securecode/threat-modeling-process-ensure-application-security_1646, 2006.*
28. J. Luna, *et al*., “A Security Metrics Framework for the Cloud,” *IEEE International Conference on Security and Cryptography (SECRYPT 2011),* 2011.
29. S. Myagmar, *et al.,* “Threat Modeling as a Basic for Security Requirements,” *Symposium on Requirements Engineering for Information Security (SREIS) in conjunction with 13th IEEE International Requirements Engineering Conference (RE), Paris, France,* 2005.
30. M. Mateski, “Cyber Threat Metrics,” *Sandia National Laboratories*, 2012.
31. S. N. Foley and W. M. Fitzgerald, “Management of Security Policy Configuration using a Semantic Threat Graph Approach,” *Journal of Computer Security (JCS)*, vol. 19, 2011.
32. A. Jones, “Identification of a Method for the Calculation of Threat in an Information Environment,” *Internal publication, QinetiQ, Inc*, 2002.
33. D. Catteddu and G. Gogben, “Security & Resilience in Governmental Clouds,” *European Network and Information Security Agency (ENISA)*, 2011.
34. C. J. Alberts, *et al.,* “Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework Version 1.0,” *Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, http://www.sei.cmu.edu/publications/documents/99.reports/99tr017/99tr017abstract.html, 1999.*
35. Amenaza, “Create Secure System through Attack Tree Modeling,” *Amenaza Technologies Limited. Internal Publication,* 2003.
36. G. Obradovic, “Threat Modeling and Data Sensitivity Classification for Information Security Risk Analysis,” *Presentation in conference on Data Protection (Dominion Volting Systems),* 2003.
37. Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0,” *Cloud Computing Alliance, http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf*, 2011.
38. Cloud Security Alliance, “Cloud Control Matrix,”. *Cloud Security Alliance, https://cloudsecurityalliance.org*, 2011.
39. John. P. P. (2006). Threat and Vulnerability Analysis: The Concept and a Methodology. http://www.interop.com/newyork/2006/presentations/conference/1087-pironti.pdf.
40. Robert. S. (2012). Cloud computing tools: Improving security through visibility and automation. *CSO Security and Risk*. www.aveksa.com/news-events/upload/Cloud-computing-tools.pdf.
41. Cloud Security Alliance. (2010). Top Threats to Cloud Computing V1.0. *Cloud Computing Alliance.* http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
42. VISTA. Presentation Study: Internet and Internal network Security Testing (Severity Levels). http://www.internetbankingaudits.com/severity_levels.htm
43. Symantec. Cloud. Threat Levels. http://www.symanteccloud.com/globalthreats.html
44. Melanie. V. (2008). A Framework towards Effective Control in Information Security Governance. *Thesis, Nelson Mandela Metropolitan University.*

BIOGRAPHY OF AUTHOR

Muhammad Imran Tariq is BCS, M.Sc Telecommunication, M.Sc Computer Science, MS Computer Science, MCSE, MCP+I, A+ and CCNA. He has 12 years teaching and administration experience in Government College of Commerce, Allama Iqbal Town, Lahore, pakistan and PIMSAT University, Lahore Campus, Pakistan. His research interests include Cloud Computing, Information Security, Wireless Networks Security and Risk Management. His previous works dealt with Wirless Security and Threats which was presented at 11th Islamic Countries Conference on Statistical Science on December 19-22, 2011 at University of Management and Technology, Lahore, Pakistan and second Designing Software Maintenance Service Level Agreement in Outsource contract which was presented at 9th International Conference on Statistical Science held on July 5-6, 2012 at NCBA&E, Lahore, Pakistan.

Moreover, at present he has been working on SLA based information security metrics in cloud computing.