International Journal of Power Control Signal and Computation (IJPCSC)
Vol. 5. No.1. pp.56-62,Jan-March 2013 ISSN: 0976-268X
www.ijcns.com

Trust Based Security Framework Model for GeoCloud

Nabil EL KADHI [#1], Walid (oualid) Ben ALI [*2]
[#] *College of IT and Design, University of Jazeera Dubai, UAE*
[1] nelkadhi@icloud.com, elkadhi.nabil@neuf.fr
[*] *MIS Department, University of Sharjah Sharjah, UAE*
[2] oali@sharjah.ac.ae

Abstract: This paper reviews the classical security services and requirements in an open environment and introduces a Trust Based Security Framework (TBSF) for cloud security. After a brief review of cloud computing security challenges, we suggest a TBSF model and we present its application for a GIS cloud based case study.

Index Terms—**Information Security, Security services, cloud computing, Trust, QoS for security, GIS, GeoCloud, Cloud security challenges.**

I. INTRODUCTION

It's an evidence how huge is the impacts of technological progress and inventions on nowadays market places and life. Computers and mainly Personal Computers have transformed the human behavior, capabilities of data processing and computing. The nineteenth have been clearly marked by the democratization of the large and wide area networks and mainly the Internet technologies.

Among all those progress, security requirements and sensitivity have increased and shifted from a mainly physical protection to data protection and data access control (mainly on 70th and 80th) then gradually to mainly communication protection and distant application management and finally e-processing of crucial data through a wide set of applications in what is nowadays called the 'Cloud'.

All those changes and progression lead to a new vague of security tools and services ranging from the data protection technique [19, 63], to the cryptographic protocol design, implementation and verification [6, 13, 14, 9]. A deep analysis of security levels and action domains allow us to distinguish the following:

- Security tools and protocols for data and communication protection [9, 42].
- Security tool for prevention [38].
- Security tools for attacks detection and logging ([44, 26, 28]).

Among all those changes and improvement the security services kept almost the same basic definitions with slight adaptation from one environment to another. As described section 2, five security services are required and aimed in any complete scurried information system.

In this paper, we argue that the newly Cloud computing and Cloud applications are introducing today a quite important paradigm shift in information security. In fact, Cloud computing as described section 3 relies on virtualization and virtual environment that may be seen as a drastic change when dealing with security tools and services. Basically, and for the first time, we need to define and specify security features independently from the applied technique, the physical layers and tools as well as the intended goals.

What is the classical view of security services? What cloud computing emergent features? What are the cloud security challenges and how we are claiming answering chose recent conditions? Those are the major questions addressed in this paper and leading to a newly defining QoS Framework for a Trust Based cloud security. We also presented how cloud computing has been used in the GIS field in order to create a new concept called GeoCloud. We described also presented a GeoCloud-based application which maps and analyzes crash data for road safety. We have shown how our Trust based cloud model is useful and can be applied in such specific context that is the geospatial one.

Our paper is structured as following. **Section 2** is a global overview of the security services and their requirements, **section 3** reviews the cloud security challenges and particularities. **Section 4** introduces the paradigm shift leading to a trust based security and introduce our QoS framework. **Section 5** details the concept of GeoCloud while **section 6** presents an application of GeoCloud. In **section 7**, we present how the Trust model is useful in the GeoCloud context before concluding **section 8**.

II. SECURITY SERVICES OVERVIEW

Specialized literature agreed on the five following required services in any Information system security solution.

- **Access control and Integrity:** One of the common definitions of integrity is that the content (of a file or a message) is as it is supposed to be after the last known authorized access. Such constraint may easily be linked to access control rules and logging when dealing with physical data protection and file and database use. It is quite different in a communication context since it refers more to the integrity and conformity between the initial (in general sent)

version and the actually checked (commonly the received) version of an exchanged message over a non private network. Various techniques are commonly applied for access control [18, 48, 50] and Integrity check values based on Hash functions [17, 60, 16]

- **Authenticity:** As well as Authentication refers to either having the proof of the identity of the communicating parties or the proof that the analyzed (received) data is as it has been sent by an already authenticated user. As we can easily notice it authenticity leads, implicitly, to integrity. A large set of cryptography based techniques are applied for authentication verification [59, 37]
- **Secrecy:** Despite the differences between Data secrecy and Information secrecy, we usually intend to ensure that a crucial content is analyzed and being interpreted in a usable way only by the legitimate users. Cryptography still the main stone when dealing with data and information secercy [51].
- **Data flow secrecy:** Commonly known as passive attacks, the data flow analysis is in fact the set of intruder actions allowing data collection regarding the attacked organization or networks. In fact, it dos the collection of include any useful information that may be used later on to build active attacks. Globally, there is no efficient data flow secrecy technique. The goal here is to lead the intruder to somehow wrong information or a non realistic environment such as done by the honey pot project [20].
- **Non repudiation:** The non repudiation is generally based on certification techniques and/or acknowledgement..[25]
- **Availability**: Availability may be defined in different context and in various manners depending on the offered services and activities. Independently, availability, in a security service context, means basically that the offered/required service is active and accessible in way ensuring that all the previous security services are respected and ensured.

III. CLOUD SECURITY CHALLENGE

After introducing the five security services elements, let's now describe how these elements are applied in Cloud Computing. To do so, we need first to define the term of Cloud Computing.

Cloud Computing has been called the *5th utility* in the line of electricity; water, telephony and gas. The reason why cloud has been called with such a name is that the cloud computing has been changing the way computer resources have been used up to now [41]. Cloud computing is the computing equivalent of the electricity as "Miller" says in his world, it's like the "revolution of a century ago" [34]. Previously, the advent of electrical utilities, in every farm and business produced its own electricity from freestanding generators. But after the electrical grid was created, all the farms and businesses shut down their generators and bought electricity from the utilities, at a much lower price and with much greater reliability than they could produce on their own. It has been shown that there are many benefits of cloud computing by virtue of abstraction, prevents the consumer from having the same level of influence over the computing resource. Great concern is the ability of consumer to assert quality of service [5]. QoS refers to aspects of a service that are not functional but are important considerations. This leads to some of the following challenges with public cloud computing. "One of the key challenges in cloud computing is data-level security" [24]. Starting with the most important challenges which are:

- (Availability)
- Then , (Data Residency),
- And, (Multitenancy),
- With, (Performance),
- (Data Evacuation),
- Ending with (Supervisory Access & Privacy)**.**

Even large enterprises with significant resources face considerable challenges at the network level of infrastructure security.

In fact, for large enterprises without significant resources, or for small to medium-size businesses (SMBs), we wonder if the risk of using public clouds (assuming that such enterprises lack the resources necessary for private clouds) is really higher than the risks inherent in their current infrastructures. In many cases, probably no—there is not a higher level of risk. In other hand, the virtualization technologies enable multitenancy cloud business models by providing a scalable, shared resource platform for all tenants. More importantly, they provide a dedicated resource view for the platform's consumers. From an enterprise perspective, virtualization offers data center consolidation and improved IT operational efficiency. Today, enterprises have deployed virtualization technologies within data centers in various forms, including OS virtualization (VMware, Xen), storage virtualization (NAS, SAN), database virtualization, and application or software virtualization (Apache Tomcat, JBoss, Oracle App Server, Web Sphere). From a public cloud perspective, depending on the cloud services delivery model (SPI) and architecture, virtualization appears as a shared resource at various layers of the virtualized service (e.g., OS, storage, database, application) [22, 24].

The simplicity of self-provisioning new virtual servers on an IaaS platform creates a risk that insecure virtual servers will be created. Secure-by-default configuration needs to be ensured by following or exceeding available industry baselines. Securing the virtual server in the cloud requires strong operational security procedures coupled with automation of procedures. Here are some recommendations:-

• Use a secure-by-default configuration. *Harden in a public cloud*.

• Track the inventory of VM images and OS versions that are prepared for cloud hosting..

• Protect the integrity of the hardened image from unauthorized access.

• Safeguard the private keys required to access hosts in the public cloud.

• In general, isolate the decryption keys from the cloud where the data is hosted—unless they are necessary for

decryption, and then only for the duration of an actual decryption activity.

• Include no authentication credentials in your virtualized images except for a key to decrypt the file system key.

• Do not allow password-based authentication for shell access [57].

IV. TRUST: A CLOUD PARADIGM SHIFT USING QOS FRAMEWORK

Among the previous sections in this paper we tried to show the gap or new challenges introduced by the cloud technology when dealing with security services. In fact, security services relays mainly on cryptography, hashing functions and a set of parameters strongly correlated to the implementation environment and the used architectures. This appears for example thru the SSL protocol handshake step or the LDAP and Kerberos implementations for authentications [35, 36]. Cloud technology comes mainly with a level of abstraction hiding internal details and implementations. Abstraction layers as introduced by several virtualization tools [27, 55] allow data mobility as well as platform independency use and code migration.

Many leaders in Cloud solutions [12, 61, 21] are today offering a global cloud environment supporting a quite complete range of security services. A highest cloud and virtualization level will allow user to migrate from one platform to another in a quite transparent way. Actually cloud platform seems to be non interoperable. And if a compatibility exists, it is en general limited to data interoperability and access. Migrating from one platform to another necessitate in general a new authentication, a new definition or paradigm shift of the security concepts definitions, costs and techniques as supported by the concerned platform. Such limitation is considered as brakes to the cloud use and reduces it is efficiency. In this section we argue that a higher abstraction is in fact required for the security services in order to introduce a more flexible cloud environment. The idea is to be detached from the classical definitions of the security services where the service verification and achievement is linked to the used techniques, the implementation method and/or the applied constraints and to support the dynamicity of the cloud environment. The paradigm shifts we are considering here intend to merge all the security services to a single one which is a **trust relationship**. Two cloud environments will trust each other regarding any of the claimed or requested security service. The trust relation is here in fact like a certificate exchanged between the two cloud environment to ensure that the required service is offered by the two parties without being obliged to decline any specific technique tool or environment. Even the idea seems to be quite sample and intuitive it does necessitate a deep analysis. In fact, assuming that a required service (let say authentication for example) is offered by two cloud environment. Shall we consider the authentication of one valid for the other? Shall we consider that the authentication requirements of the two parties are compatible? This may or may not be the case depending on several conditions and contexts. It is of course unacceptable to check different conditions and constraints as many times as a virtual environment is changing. The key solution here is to replace such challenging condition by an abstraction where only simple verification is required. If we look deeply to the authentication requirements (as in our actual example) we are in fact not caring much more about the used technique, the key size and the certification authority than the hardness, level or quality of the offered authentications in any environment. So if the two environment require a simple authentication or a strong one and if there is a third party to classify and certify the authentication level of each party, without deeply detailing the used techniques, the two parties will be able to 'trust' each other regarding the authentication even if they are using various virtualization platform and security techniques.

The additional challenge here is that the 'trust' relation and if we assume that it has been established initially, it must be guaranteed among all the cloud dynamicity and physical environment changes. Each party will have and additional challenge which is having an adaptable dynamic certificate that guarantee that the 'trust' relation is active when changing any cloud environment component. QoS contracts are a suitable tool to ensure a continually verified set of conditions and rules.

A. *Trust between PaaS Platforms in the clouds*

The trust relation in clouds requires a kind of certificate exchanged between the two clouds environment to ensure that the required service is offered by the two parties. Before that we should clarify the trust concept and know the Components of trust in Cloud Computing.

The Trust can be explained in diverse fields such as psychology, sociology, and economics. Also trust can be classified in different meaning for many writers. But In dictionaries and other authors, trust is generally related to "levels of confidence in something or someone" [7, 40, 30].

The classified trust which is used in Peer to Peer networks (for example) is identified and described following;

1- CuboidTrust,
2- EigenTrust,
3- Bayesian Network based Trust Management (BNBTM),
4- GroupRep,
5- AntRep,
6- Semantic Web,
7- Global Trust,
8- PeerTrust,
9- comPrehensive reputAtion-based TRust mOdeL with Fuzzy subsystems (PATROL-F),
10- Trust Evolution,
11- Time-based Dynamic Trust Model (TDTM)
12- Trust Ant Colony System (TACS

The main *components affecting cloud trust* are:

1) Security: Mechanisms (e.g. encryption) which make it extremely difficult or uneconomical for an unauthorized person to access some information [23, 40].

2) Privacy: Protection against the exposure or leakage of personal or confidential data (e.g. personally identifiable information (PII)).[7]

3) Accountability: Defined as "the obligation and/ or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations".

4) Auditability: The relative ease of auditing a system or an environment. Poor auditability means that the system has poorly-maintained (or non-existent) records and systems that enable efficient auditing of processes within the cloud. Audit ability is also an enabler of (retrospective) accountability "It allows an action to be reviewed against a pre-determined policy to decide if the action was compliant", and if it was not, to hold accountable the person or organization responsible for the action.[40,62]. The Framework [49, 50].of trust in cloud is as shown in figure 1.

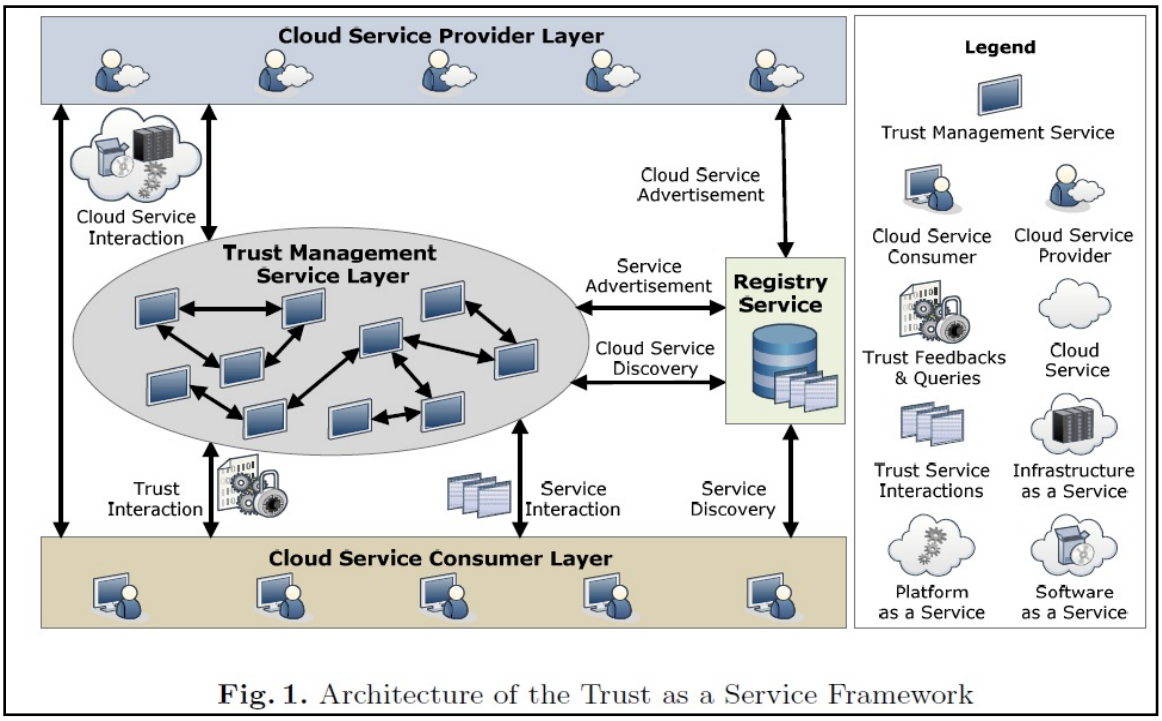

Fig. 1. Architecture of the Trust as a Service Framework

V. THE GEOCLOUD

Geographic Information Systems (GIS) applications are generally both computer and data intensive in nature. GIS technology has been around for decades. These mature technologies are increasingly using geo-spatial and non-spatial data. Advance data collection technologies have facilitated large amounts of rich data to be collected at diverse data sources. In time, size of the data would grow to be large enough to restrict any single organization to maintain and handle these data. In addition, GIS functions and services that operate on these data are geographically and logically distributed due to the source of data, location of computing facilities and organizations. The spatial analysis on large amount of data is complex and computationally intensive [6-G]. In order to share and collaborate GIS data and the computational results among geographically dispersed users, a scalable and low cost computation platform, such as cloud computing- is required for GIS applications. As result, a new technology called GeoCloud has emerged [54-G]. In the next section, we present how the GeoCloud is used to develop a GIS-cloud based application related to the crash data analysis.

A. GeoCloud application: The case of crash data analysis application

The main objective of this applied research is to take advantages of the cloud technology and apply it in the development of a cost effective GIS-based application which will help the police department to map and analyze crash data

in order to increase road safety. This application combines many types of data, spatial and non-spatial, to derive meaningful information. In order to develop this application an ESRI cloud system (for spatial data such as crash location) and Oracle database hosted in a cloud (for non spatial data such as demographic data about the drivers and non-spatial crash data) have been used. The architecture of this application is presented in Fig. 2. In this architecture, we can see that the application relies on several heterogeneous cloud systems at the same time.

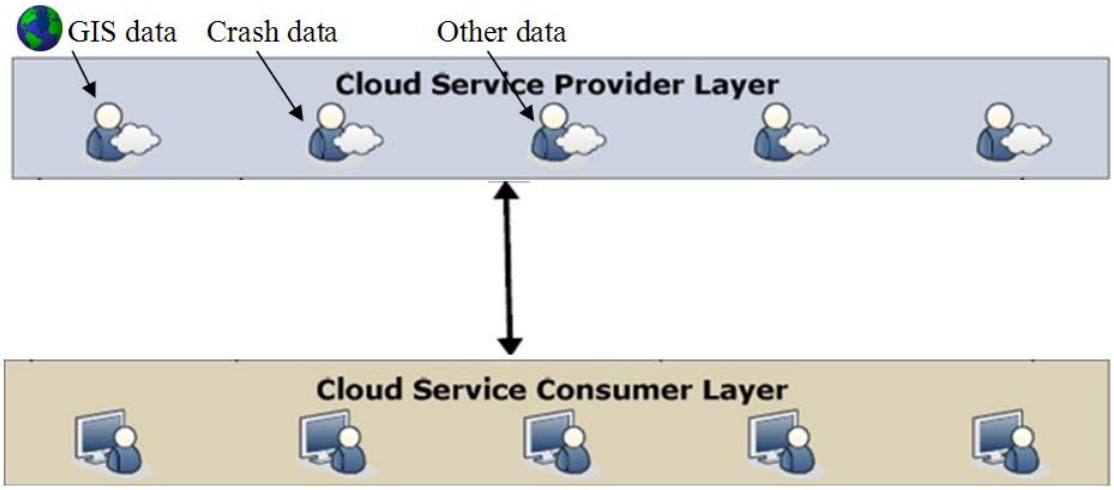

Fig. 2. Cloud architecture of the GIS-based crash data analysis application

B. *The application of the Trust Based Security Framework model to the GeoCloud*

In the previous section, we have presented a GIS-based application which benefits from the cloud technology in order to map and analyze crash data. It has been shown that this application uses many cloud systems. These systems are heterogeneous, since some of them contains spatial data, others contains non-spatial data, others systems contains analysis functions and routines, etc. In order to fulfill the complete function of the systems, these clouds should exchange data between them. As everybody knows, most o the GIS data, and especially, our application's data are very confident, so the communication between the clouds should be secured. The heterogeneity of these clouds, as well as the confidentiality of the manipulated data, present good arguments to use our presented TBSF model to secure the communications between the clouds.

VI. CONCLUSIONS

In this paper we have presented the important of information security in cloud environments. We justify the utility and need for a new paradigm shift in cloud security and we suggest a trust based model. QoS concepts and specification are choosen as implementation technique for the Trust based model. Even though we did not include any specification of the required QoS we have been showing how such model can be applied in various domains and applications such as GeoCloud and particularly to a specific crash data analysis use. The suggested model showed a huge degree of flexibility and we have been able to customize it easily to a GeoCloud context. We are actually exploring other Cloud applications in order to test our TrustModel portability and to develop a set of abstract primitives that allow implementing it in various contexts with an acceptable customization effort.

References.

1. Aidan Finn, Hans Verdevoort, Patrick Lownds, and Damian Flynn, Microsoft Private Cloud Computing - (Jun 26 , 2012).

2. Anthony T. Velte, Toby Velte, Robert Elsenpeter, Cloud Computing A Practical Approach, Mc Graw Hill Companies, ISBN: 978-0-07-162695-8, Edition – 2010.

3. Barrie Sonsinsky , Cloud computing Bible , (Jan 11, 2011).

4. Ben Halpert, (2011), "Auditing Cloud Computing",(pp: 02); United State Of America/Library of Congress Cataloging.

5. Ben Halpert, (2011), "Auditing Cloud Computing",(pp: 10-12);United State Of America/Library of Congress Cataloging.

6. Bicarregui, J.C. and Matthews, B.M.; Formal Methods in Practice: A Comparison of Two Support Systems for Proof, SOFSEM '95: Theory and Practice of Informatics, Editions Springer-Verlag 1995,

6-G Bhat, Razeef Mohd Shah, Bashir Ahmad, Cloud Computing: A solution to Geographical Information Systems

(GIS). International Journal on Computer Science and Engineering (IJCSE). Vol. 3, No.2, 2011

7. Changhoon Lee, Jean Marc Seigneur, James J. Park and Roland R. Wagner, Secure and Trust Computing, Data Management, and Applications: STA 2011 Workshops: IWCS 2011 and STAVE 2011, Loutraki, Greece, Jun 28-30.2011, in computer information science, (Nov 4, 2011).

8. Charles Babcock, Management Strategies for the cloud Revolution: How Cloud Computing Is Transforming Business and Why /you Can't Afford to Be Left Behind – (Apr 16, 2010).

9. CISCO, http://www.cisco.com. Accessed March 2008

10. David Patterson and Armando Fox , Engineering Long-Lasting Software: An Agile Approach Using SaaS and Cloud Computing, Alpha Edition (Jan 12, 2012).

11. Don Peppers, Managing Customer Relationship: A Strategic Framework – (Jan 11,2011).

12. Edward Haletky, VMware vSphere and Virtual Infrastructure Security: Securing the Virtual Environment, (Jul 2, 2009).

13. EL Kadhi, N and H. EL Gendy, Advanced Method for Cryptographic Protocol Verification, Journal of Computational Methods in Sciences and Engineering, Volume 6, Issue 5, Supplement 1, Year 2006, Pages: 109-119

14. EL Kadhi, N, Hadjar, K and EL Zant, J, A Mobile Agents and Artificial Neural Networks. For Intrusion Detection, JOURNAL OF SOFTWARE, VOL. 7, NO. 1, JANUARY 2012

15. Eugenio Pace, Moving Application to the Cloud on the Microsoft Azure Platform (Patterns & Practces)- (Sep 6 , 2010).

16. FIPS PUB 180-1, Supersedes FIPS PUB 180, SECURE HASH STANDARD, 1993 May 11

17. Gene Tsudik, "Message Authentication with one-way Hash Functions", ACM SIgcom 1992

18. Gopalakrishnan, M. & Patnaik, L.M Medium access Control Schemes for Local Area Networks with Multiple Priority" Function, the computer journal, vol 31 N°3 1988

19. Goscinski, Andrzej, Distributed Operating Systems, The Logical Design. Addison-Wesley 1991

20. Hone ypot Project: http://projecthoneypot.org/

21. James Beswick, Google Apps Express: The Fast Way To Start Working in the Cloud , (Mar 5, 2011).

22. Joel Scott, Microsoft CRM for Dummies – (Jul 25, 2003).

23. John Townsend , Beyond Boundaries: Learning to Trust Again in Relationships (Sep 27, 2011).

24. John W. Rittinghouse and James F. Ransome, (2009), "Cloud Computing: Implementation, Management, and Security", New York, Auerbach Publications.

25. Jose A. Onieva, Secure Multi-Party Non-Repudiation Protocols and Applications (Advances in Information Security (Dec 8, 2010).

26. K. Deeter, K. Singh, S. Wilson, L. Filipozzi and S. Vuong, APHIDS: A Mobile Agent-Based Programmable Hybrid , Intrusion Detection System, in Mobility Aware Technologies and Applications. LNCS, vol. 3284, (Springer, Heidelberg, 2004).

27. Kenneth Hess and Joe Brockmeier, Practical Virtualization Solutions: Virtualization from the Trenches , (Oct 22, 2009).

28. Ktata, F, EL Kadhi, N and Ghedira K. MAFID Agent IDS Based on Missuse Approach, Journal Name: Journal of Software, Volume 4 Number 6 Year 2009, Pages: 495-507, ISSN 1796-217X, ACADEMIC PUBLISHER

29. Lars Nielsen, The little Book of cloud computing , 2011 Edition (Apr 11, 2011).

30. Lars Nielsen, The little book of cloud computing security - Edition (Dec 18,2011).

31. Lvanka Menken, Cloud Computing PaaS Platform and Storage Management Specialist Level Complete Certification Kit – Platform as a Service Study Guide Book and Online – Certification Sepcialist – Second Edition (Aug 20, 2010).

32. Manuel, P., Thamarai Selvi, S., Barr, M.E.: Trust Management System for Grid and Cloud Resources. In: Proc. of ICAC 2009, Chennai, India (December 2009).

33. Martin Hingley, (September 21, 2011), "UK Cloud Computing Forecast Highlights", (UK Cloud Computing Forecast – Recession-Busting Growth), available at (http://itcandor.net/2011/09/21/cc-uk-q311/).

34. Michael Miller, (2009) ," Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online",(pp: 07,08,09); United State Of America/Library of Congress Cataloging.

35. MIT, Kerberos, 'Kerberos: The Network Authentication Protocol, available at (http://web.mit.edu/Kerberos/)

36. MIT , Kerberos: K'Kerberos Security Advisories. Available at (http://web.mit.edu/Kerberos/advisories/)

37. Needham, R. M. and Schroeder, Michael D., Using Encryption for Authentication in Large Networks of Computers, Communications of the ACM}, V 21, Number CSL-78--4}, December 1978.

38. Nitesh Dhanjani and Justin Clarke, Network Security Tools: Writing Hacking and Modifying Security Tools, Apr 11, 2005

39. Open Trust Security is about Trust, (2012), available at (http://www.opentrust.com/en/saas).

40. Qing Zhang, Ting Yu, and Keith Irwin, "A Classification Scheme for Trust Functions in Reputation-Based Trust Management," in International Workshop on Trust, Security, and Reputation on the Semantic Web, Hiroshima, Japan, 2004.

41. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility, Future Generation Computer Systems, Volume 25, Number 6, Pages: 599-616, ISSN: 0167-739X, Elsevier Science, Amsterdam, The Netherlands, June 2009.

42. RealSecure, http://www.iss.net. Accessed March 2008.
43. Russell Dean Vines and Ronald L. Krutz - Cloud Security : A Comprehensive Guide to Secure Cloud Computing - (Aug9, 2010).
44. S. Specht and R. Lee, Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures, in Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, (September 2004).

45. Scott Lowe, Mastering Vmware v Sphere 5 - Oct 18, 2011).
46. Search Cloud Computing , (December 2007), available at (http://searchcloudcomputing.techtarget.com/definition/cloud-computing).
47. SHEA, G.O , Controlling the Dependencyof User access Control Mechanisms on correctness of User Identification, The Computer Journal vol 31 N° 6 1988

48. Sheth, A.P., Gomadam, K., Lathem, J.: SA-REST: Semantically Interoperable and Easier-to-Use Services and Mashups. IEEE Internet Computing 11(6), 84–87 (2007).

49. Shiu-Kai Chin and Susan Beth Older, Access Control, Security, and Trust: A Logical Approach (Chapman & Hall/CRC Cryptography and Network Security Series, 2010.
50. Shneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, Paperback , 1996
51. Sims, K. (2009), 'IBM Blue Cloud Initiative Advances Enterprise Cloud Computing' – available at http://www-03.ibm.com/press/us/en/pressrelease/26642.wss .

52. Stefan Ried, (April 21, 2011), "Sizing the Cloud", (For Vender Strategy Professional Blog), available at (http://blogs.forrester.com/stefan_ried/11-04-21-sizing_the_cloud).
53. Stephen R Smoot , Private Cloud Computing : Consolidation, Virtualization, and Service-Oriented Infrastructure - (Oct 29, 2011).
54-g Suraj Pandey, Cloud Computing Technology & GIS Applications, The 8th Asian Symposium on Geographic Information Systems From Computer & Engineering View (ASGIS 2010), ChongQing, China, April 22-24, 2010.
54. Talal H. Noor and Quan Z. Sheng, Trust as a Service: A Framework for Trust Management in Cloud Environments, School of Computer Science,The University of Adelaide, Adelaide SA 5005, Australia.
55. Tim Mather, Subra Kumaraswamy, and Shahed Latif - Cloud Security and Privacy – (September 2009).
56. Timothy Chou, Introduction to Cloud Computing(in about 1,000 words) (Dec 27, 2010).
57. Todorov, D. Mechanics of User Identification and Authentication: Fundamentals of Identity Management, Dob, HardCover, June 2007.
58. Tony Guidici and Tejaswi Redkar, Windows Azure Platform , (Dec 7 , 2011).
59. Tsudik, Gene, Message Authentication with One-Way Hash Function, Computer Communication Review, 1992,
60. Types of Cloud Computing, available at (www.thecloudtutorial.com).
61. Vic j.R Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics - (Apr 29.2011).
62. William Stalling & Laxrie Brown 'Computer Security Principals and Practices' Pearson Edition 2008.
63. Yong Wang, Vinny Cahill, Elizabeth Gray, Colin Harris, and Lejian Liao, "Bayesian network based trust management," in Autonomic and Trusted Computing. Berlin / Heidelberg: Springer, 2006, pp. 246-257.