**International Journal of Management, IT & Engineering**
Vol. 8 Issue 5, May 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

# A STUDY ON SECURING OF DATA IN CLOUD COMPUTING

***[1] AKASH AHMAD BHAT , [2] DR. SYED MASAID ZAMAN***

*[1] Department of Computer Science Shri Venkateshwara University, Gajrula-U.P India*

*akashmajeedbhat@gmail.com*

*[2] Department of Information Technology Shri Venkateshwara University, Gajrula-U.P India*

*dr.syedmasaid@gmail.com*

***Abstract:***

*Cloud computing provides services on demand to its users. The data storage is among one of the basic services provided by the cloud computing. Cloud computing is the combination of many existing technologies that have developed at different rates and in different contexts. The main objective of cloud computing is to allow its users to take maximum benefit from all these technologies. Most of the well known organizations are moving into cloud because it allows the users to store their data on clouds and can access at anytime from anywhere whenever needed. Cloud computing can play a pivotal role in any n disaster whether natural or anthropogenic in the fields of education, health, business and other allied sectors. The data from different users and business organizations are together in cloud, there is a every possibility of data breaching in cloud environment by transferring the data to the cloud, mainly the data owners shift the control of their data to other person that may raise security breaches and threats. Many of times the Cloud Service Provider (CSP) itself may corrupt the data illegally. As we know that the data owners and servers are different identities, the paradigm of data storage brings up many security concerns. An independent method is the order of the day in order to store the data efficiently in to cloud storage server (CSS). In this paper, we will discuss the different techniques and methods that are used to overcome the security concerns while storing the data on cloud.*

**Keywords:** Cloud computing, Data storage, CSS, CSP, Security Threats, Data Breaching.

## INTRODUCTION

From the past decade or so, there has been a tremendous progress in Cloud Computing. Cloud Computing delivers a exclusive and wide range of resources like computational power, computational platforms, data storage and applications to the users by the medium of internet. With a large number of companies resorting to use exclusive resources in the Cloud, there is a foremost necessity for protecting the data of users. Some major existing and upcoming challenges that are being faced by Cloud Computing are security, protection and process the data which is the exclusive property of the user. Below, we have mentioned in detail the two main states that hold the data is out in the Cloud: when the data is in transition process and when the data is static, where the data is expected to be very much secure. The below illustrated are the two main scenarios which we have mainly focused to understand the security of the data in the Cloud.

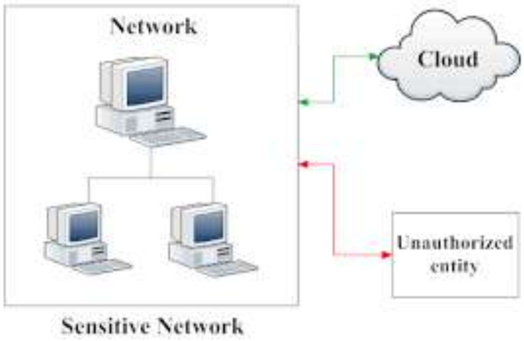


Figure 1.1 Unauthorized access of data between the network and Cloud

The above figure 1.1 describes a scenario where a local network is connected to a Cloud network, in which some part of the network data is broken out from the local network and placed in the Cloud, but the critical data resides in the local network itself. In this case, the Cloud provider does not have any privilege of accessing the data physically which is in the local network. But in some cases, the Cloud needs to access some information which is in the local network, during that access; there exists a possibility of unauthorized access of the local network resources. It describes the typical problem in network security where the information can face active attacks and passive attacks. The active attacks include masquerading, replay attack, modification of messages and denial of service. Passive attacks include traffic analysis. These attacks are likely to happen when the stream of information leaves the client network to the Cloud network.

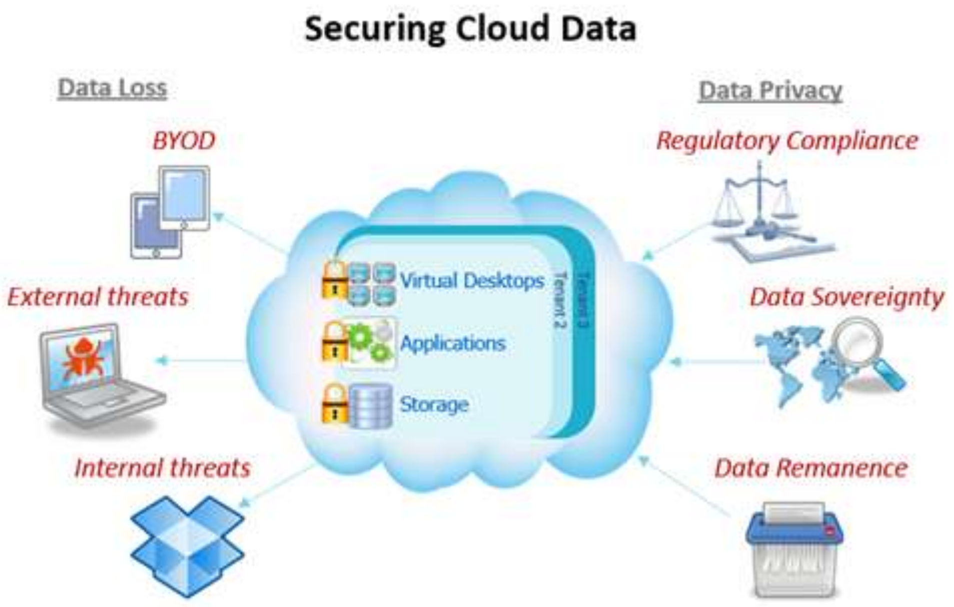


Figure 1.2 Unauthorized access of data within the Cloud

The above figure 1.2 describes the scenario where the total data of the local network resides within the Cloud, where the local network and the authorized users can access their data physically in the Cloud. At that instant of time, there exists a possibility for unauthorized users to enter and access the data in the Cloud. In this situation, the virtual machines are allotted to users of the Cloud. These machines have valid logins. However, these logins can be abused and cracked. The data may also be accessed in other perverted ways. Regarding this area of study, most of the research papers followed a normal traditional literature survey method. Few papers gave an innovative idea and proposed a security model. However, there are very few works, which considered the opinions of various security experts in Cloud Computing. This study proposes that, reader gets the true reflection of the security practices followed by various Cloud Computing companies in the current era. There are very few papers which focus on the security techniques for specified applications. In the increasingly prevalent cloud computing, datacenters play a fundamental role as the major cloud infrastructure providers, such as Amazon, Google, and Microsoft Azure. Datacenters provide the utility computing service to software service providers who further provide the application service to end users through Internet. The later service has long been called "Software as a Service (SaaS)", and the former service has recently been called "Infrastructure as a Service (IaaS)", where the software service provider is also referred to as cloud service provider. To take advantage of computing and storage resources provided by cloud infrastructure providers, data owners outsource more and more data to the datacenters through cloud service providers, e.g., the online storage service provider, which are not fully trusted by data owners. As a general data structure to describe the relation between entities, the graph has been increasingly used to model complicated structures and schema less data, such as the personal social network (the social graph), the relational data base, For the protection of users’ privacy, these sensitive data have to be encrypted before outsourcing to the cloud. Moreover, some data are supposed to be shared among trusted partners to all organizations. There have been publicized attacks on cloud computing providers and this paper discusses recommended steps to handle cloud security, issues to clarify before adopting cloud computing, the need for a governance strategy and good governance technology, cloud computing strengths, weaknesses, analyzes the benefits and cloud computing information security management. This paper has discussed some of the services being provided.

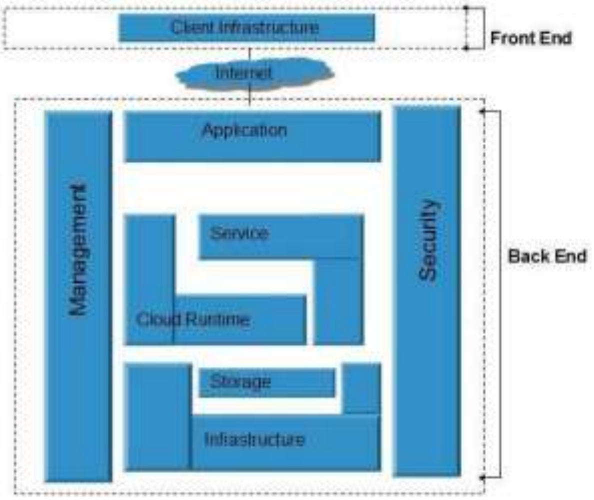
## Cloud computing architecture

Cloud computing architecture refers to the components and subcomponents required for cloud computing. These components typically consist of a front end platform (fat client, thin client, mobile device), back end platforms (servers, storage), a cloud based delivery, and a network (Internet, Intranet, Intercloud). Combined, these components make up cloud computing architecture.

Cloud Computing architecture comprises of many cloud components, which are loosely coupled. We can broadly divide the cloud architecture into two parts:

- Front End
- Back End

Each of the ends is connected through a network, usually Internet. The following diagram shows the graphical view of cloud computing architecture:



### Front End

The **front end** refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, Example - Web Browser.

### Back End

The **back End** refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

Note

- It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols.
- The server employs certain protocols known as middleware, which help the connected devices to communicate with each other.

### Software as a service (SaaS)

The software-as-a-service (SaaS) service-model involves the cloud provider installing and maintaining software in the cloud and users running the software from cloud over the Internet (or Intranet). The users' client machines require no installation of any application-specific software since cloud applications run in the cloud. SaaS is scalable, and system administrators may load the applications on several servers. In the past, each customer would purchase and load their own copy of the application to each of their own servers, but with the SaaS the customer can access the application without installing the software locally. SaaS typically involves a monthly or annual fee.

Software as a service provides the equivalent of installed applications in the traditional (non-cloud computing) delivery of applications.

Software as a service has four common approaches:

1. single instance
2. multi instance
3. multi-tenant
4. flex tenancy

Of these, flex tenancy is considered the most user adaptive SaaS paradigm in designated multi-input four way manifold models. Such systems are based on simplified encryption methods that target listed data sequences over multiple passes. The simplicity of this concept makes flex tenancy SaaS popular among those without informatics processing experience, such as basic maintenance and custodial staff in franchise businesses.

**Development as a service (DaaS)**

Development as a service is web based, community shared tool set. This is the equivalent to locally installed development tools in the traditional (non-cloud computing) delivery of development tools.

**Data as a service (DaaS)**

Data as a service is web based design construct where could data is accessed through a defined API layer. DaaS services are often considered as a specialized subset of a Software as a Service (SaaS) offering.

### Platform as a service (PaaS)

Platform as a service is cloud computing service which provides the users with application platforms and databases as a service. This is equivalent to middleware in the traditional (non-cloud computing) delivery of application platforms and databases.

### Infrastructure as a service (IaaS)

Infrastructure as a service is taking the physical hardware and going completely virtual (e.g. all servers, networks, storage, and system management all existing in the cloud). This is the equivalent to infrastructure and hardware in the traditional (non-cloud computing) method running in the cloud. In other words, businesses pay a fee (monthly or annually) to run virtual servers, networks, storage from the cloud. This will mitigate the need for a data center, heating, cooling, and maintaining hardware at the local level.

## THREATS IN CLOUD COMPUTING

With an estimated 70% of all organizations using the cloud, cloud security threats should be a concern for every business. A 2017 study by CGI and Oxford Economics measured the costs resulting from data breaches in the last five years at more than $50 billion, according to a Fortune article.The cloud provides a flexible model for simplified IT management, remote access, mobility, and cost-efficiency. But as more mission-critical applications migrate to the cloud, data privacy and software security are growing concerns.Moving web applications to the cloud does not make them inherently more secure. Your organization might be ready to embrace the benefits of the cloud infrastructure. But you must also ensure you address all the potential security risks in cloud computing.Cloud computing provides many advantages, such as speed and efficiency via dynamic scaling. But there are also a host of potential threats in cloud computing. These cloud security threats include data breaches, human error, malicious insiders, account hijacking, and DDoS attacks. In fact, a Ponemon Institute study indicated that overall, a data breach was three times more likely to occur for businesses that use the cloud than for those that don't.Here's a list of the 10 most critical cloud security threats you face. We've also described the steps you should take when choosing cloud computing technologies and providers.

SYNOPSYS
10 Critical Cloud Security Threats in 2018 and Beyond
1. Data breaches
2. Human error
3. Data loss with no backup
4. Insider threats
5. DDoS attacks
6. Insecure APIs
7. Exploits
8. Account hijacking
9. Advanced persistent threats
10. Spectre & Meltdown
Next step: Develop a cloud provider due diligence checklist
SYNOPSYS

SYNOPSYS
10 Critical Cloud Security Threats in 2018 and Beyond
1. Data breaches
2. Human error
3. Data loss with no backup
4. Insider threats
5. DDoS attacks
6. Insecure APIs
7. Exploits
8. Account hijacking
9. Advanced persistent threats
10. Spectre & Meltdown

1. **Data breaches.** The risk of a data breach is not unique to cloud computing, but it consistently ranks as a top concern for cloud customers.
2. **Human error.** According to Jay Heiser, research vice president at Gartner, "Through 2020, 95% of cloud security failures will be the customer's fault."
3. **Data loss with no backup.** An accident or catastrophe can lead to the permanent loss of customer data unless there are measures in place to back up that data.

4. **Insider threats.** A recent research report noted, "53% of organizations surveyed confirmed insider attacks against their organization."
5. **DDoS attacks.** Distributed denial-of-service attacks pose significant risks to cloud customers and providers, including lengthy service outages, reputational damage, and exposure of customer data.
6. **Insecure APIs.** As the public "front door" to your application, an API is likely to be the initial entry point for attackers. Use pen testing to uncover security weaknesses in the APIs you use.
7. **Exploits.** The multitenancy nature of the cloud (where customers share computing resources) means shared memory and resources may create new attack surfaces for malicious actors.
8. **Account hijacking.** Using stolen credentials, attackers may gain access to critical areas of cloud computing services, compromising the confidentiality, integrity, and availability of those services.
9. **Advanced persistent threats.** Many advanced persistent threat groups not only target cloud environments but use public cloud services to conduct their attacks.
10. **Spectre & Meltdown.** Attackers can exploit Meltdown to view data on virtual servers hosted on the same hardware, potentially disastrous for cloud computing hosts. Spectre is even worse—harder to exploit, but harder to fix too

## CLOUD COMPUTATION IMPLEMENTATION GUIDELINES

Steps to Cloud Security

Edwards (2009) stated that, with the security risk and vulnerability in the enterprise cloud computing that are being discovered enterprises that want to proceed with cloud computing should, use the following steps to verify and understand cloud security provided by a cloud provider:

Understand the cloud by realizing how the cloud's uniquely loose structure affects the security of data sent into it. This can be done by having an in-depth understanding of how cloud computing transmit and handles data.

Demand Transparency by making sure that the cloud provider can supply detailed information on its security architecture and is willing to accept regular security audit. The regular security audit should be from an independent body or federal agency. Reinforce

Internal Security by making sure that the cloud provider's internal security technologies and practices including firewalls and user access controls are very strong and can mesh very well with the cloud security measures.

Consider the Legal Implications by knowing how the laws and regulations will affect what you send into the cloud.

Pay attention by constantly monitoring any development or changes in the cloud technologies and practices that may impact your data's security.

## ISSUES TO CLARIFY BEFORE ADOPTING CLOUD COMPUTING

The world's leading information technology research and advisory company, has identified seven security concerns that an enterprise cloud computing user should address with cloud computing providers (Edwards, 2009) before adopting:

User Access. Ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information. Major Companies should demand and enforce their own hiring criteria for personnel that will Operate heir cloud computing environments.

Regulatory Compliance. Make sure your provider is willing to submit to external Audits and security certifications.

Data location. Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the privacy rules of those Jurisdictions.

Data Segregation. Find out what is done to segregate your data, and ask for proof that encryption schemes are deployed and are effective.

Disaster Recovery Verification. Know what will happen if disaster strikes by asking whether your provider will be able to completely restore your data and service, and find out how long it will take. Disaster Recovery. Ask the provider for a contractual commitment to support specific types of investigations, such as the research involved in the discovery phase of a lawsuit, and verify that the provider has successfully supported such activities in the past. Without evidence, don't assume that it can do so.

Long-term Viability. Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application.

## SOLUTION OF SECURITY ISSUES

Find Key Cloud Provider:- First solution is of finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.

Clear Contract: Contract with cloud vendor should be clear. So if cloud vendor closes before contract, enterprise can claim.

Recovery Facilities Cloud vendors should provide very good recovery facilities. So, if data are fragmented or lost due to certain issues, they can be recovered and continuity of data can be managed.

Better Enterprise Infrastructure Enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber attacks.

Use of Data Encryption for security purpose Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor. IT leaders must define strategy and key security elements to know where the data encryption is needed.

Prepare chart regarding data flow There should be a chart regarding the flow of data. So the IT managers can have idea where the data is for all the times, where it is being stored and where it is being shared. There should be total analysis of data.

## CONCLUSION

Cloud computing is a combination of several key technologies that have evolved and matured over the years. Cloud computing has a potential for cost savings to the enterprises but the security risk are also enormous. Enterprise looking into cloud computing technology as a way to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing. The strength of cloud computing in information risk management is the ability to manage risk more effectively from a centralize point. Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. We tried to solve many issues. In our future work, we will include the developing of testing of data flow and security in cloud computing.

## FUTURE WORK

We are investigating in the cloud security management problem. Our objective is to block the hole arise in the security management processes of the cloud consumers and the cloud providers from adopting the cloud model. To be able to resolve such problem we need to Capture different stakeholders security requirements from different perspectives and different levels of details map security requirements to the cloud architecture, security patterns and security enforcement mechanisms and Deliver feedback about the current security status to the cloud providers and consumers. We propose to adopt an adaptive model-based approach in tackling the cloud security management problem. Models will help in the problem abstraction and the capturing of security requirements of different stakeholders at different levels of details. Addictiveness will help in delivering an integrated, dynamic and enforceable cloud security model. The feedback loop will measure the security status to help improving the current cloud security model and keeping cloud consumers aware with their assets' security status (applying the trust but verify concept)

## *REFERENCES*

- *Ahmed S, Raja M. (2010) 'Tackling Cloud security issues and forensics model', High Capacity Optical Networks and Enabling technologies (HONET) , 19-21 Dec, pp. 190-195.*

- *Ahuja R. (June 2011) 'SLA Based Scheduler for Cloud storage and Computational Services', International Conference on Computatonal Science and Applications (ICCSA), 258-262.*
- *Albeshri A, Caelli W. (Sept 2010) 'Mutual Protection in a Cloud Computing Environment', 12th IEEE International Conference on High performance Computing and Communications (HPCC), 641-646.*
- *Almulla S, Chon Yeob Yeun. (March 2010) 'Cloud Computing Security management ', 2nd International Conference On Engineering Systems Management and Its Applications , 1-7.*
- *Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems; 2009; 25(6):599–616.*
- *Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A View of Cloud Computing. Communications of the ACM ; 2010; 53(4):50–58.*
- *Subashini S, Kavitha V. A survey on security i ssues in service delivery models of cloud computing. Journal of Network and mputer Applications; 2011; 4(1):1–11.*
- *Takabi H, Joshi J B D, Ahn G. Security a nd privacy challenges in cloud computing environments. IEEE Security & Privacy;2010;8(6) :24–31.*
- *Sangroya A, Kumar S, Dhok J, Varma V. Towards analyz ing data security risks in cloud computing environments. Communications in Computer and Information Science; 2010; 54 :255–265.*
- *Boss G, Malladi P, Quan D, Legre gni L, Hall H. Cloud computing, 2009. h ttp://www.ibm.com/developerswork/websphere /zones/hipods/ library.html.*
- *Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing (Draft). NIST. 2011. http://www.productionscale.com/home/2011/8/7/the-nist-definition-of-cloudcomputingdraft.html#axz z1X0xKZRuf.*
- *Cloud Security Alliance. Security gui dance for critical areas of focus in cloud computing(v2.1). Decemeber, 2009.*
- *Pearson, S. and Azzedine Benameur, “Privacy, Security and Trust Issues Arising from Cloud Computing” in 2010 IEEE Second International Conference Cloud*

*Computing Technology and Science (CloudCom),Nov 30-Dec 3,2010, page(s): 693-702.*

- *Jinzhu Kong, "A Practical Approach to Improve the Data Privacy of Virtual Machines" 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), June 29 -July 1 ,2010, pp. 936-941.*
- *Esteves, R.M. and Chunming Rong, "Social Impact of Privacy in Cloud Computing" in 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), N ov. 30-Dec. 3 ,2010, pp. 593-596*
- *Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online Michael Miller*
- *Cloud Application Architectures: Building Applications and Infrastructure in the Cloud (Theory in Practice) by George Reese.*
- *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) by Tim Mathe*
- *Dot Cloud: The 21st Century Business Platform Built on Cloud Computing Peter Fingar*
- *Ramanujam, S., Gupta, A., Khan, L., & Seida, S(2009). R2D: Extracting relational structure from RDF stores. In Proceedings of the ACM/IEEE International Conference on Web Intelligence, Milan, Italy*
- *Smith, S., & Weingart, S. (1999). Building a high performance, programmable secure coprocessor [Special Issue on Computer Network Security]Computer Networks, 31, 831–860. doi:10.1016 S1389-1286(98)00019-X*
- *Teswanich, W., & Chittayasothorn, S. (2007). ATransformation of RDF Documents and Schemascto Relational Databases. IEEE Pacific Rim Conferences on Communications, Computers, and Signal Processing,38-41.*
- *https://www.synopsys.com/blogs/software-security/10-cloud-security-threats-2018/*
- *B. lagesse. (Mar.2011) 'Challenges in Securing the Interface between the cloud and Pervasive Systems', 2011 IEEE International Conference on Pervasive Computing and Communications Workshops, 106-110.*
- *Brenner Michel, Wiebelitz Jan. (may 31, 2011) 'Secret program execution in the Cloud applying homomorphic encryption', Digital Ecosystems and Technologies Conference (DEST), 5th IEEE InternationalConference2011,114-119.*

- *Sravan Kumar R, Saxena A. (jan 2011) 'Data Integrity proofs in Cloud storage', Communication Systems and networks (COMSNETS), Third International Conference 2011, 1-4.*