International Journal of Security and Its Applications
Vol. 11, No. 12 (2017), pp.1-14
http://dx.doi.org/10.14257/ijsia.2017.11.12.01

Security and Trust In Cloud Computing: A Survey

Fatmeh Sedaghat, Majid Haghparast* and Mehrdad Maeen

Department of Computer Engineering, Yadegar-e-Imam Khomeini (RAH) Shahre Rey Branch, Islamic Azad University, Tehran, Iran
**haghparast@iausr.ac.ir*

Abstract

Cloud computing is a model which pays to easy availability, distributed and comprehensive aggregation computing resources and configurable common computing. In cloud computing, abilities based on information technology can be accessible as the service that doesn't need accurate knowledge based on structural technologies and with less management effort. Regarding to this, one of the most important issues will be the security issue for novel technologies. So we tried to review these security affairs and we emphasize that even there are several security enhancement approaches, but a comprehensive cloud computing approach should be presented in IT world. Availability of data and information privacy and services in cloud computing area cannot solve the security of cloud computing and new strategies and technologies should be used together for protection of total system. The data security and privacy issue in cloud environment is more important rather than the usual network because the information in cloud computing environment is significantly related to the network and server. In this regard these problems had been caught up the enhancement in cloud computing area and also security affairs are considered as the main problem.

Keywords*: Cloud computing, security, privacy, trust*

1. Introduction

We can mention that, United State National Information Systems Security (INFOSEC) had been defined the "security in information systems" as the systems protection against unknown access or alteration of information for storage, processing, or against the refutation of attacks in service, including the necessary determination of what should be detected, document, and threats [1]. Meanwhile we can mention other definitions of data security such as US Code Title 44, there is an appropriate definition for reaching integrity, meaning as the guarantee for protection against illegal modification of data; privacy, protection against illegal revelation of data; availability. Nowadays, operations and processes are redefined by using of data security. Systems store lots of valuable information about clients and customers and new products [2]. To recognize this concept, some routine examples caused by security, inappropriate security settings, configurations, procedure can be mention as the following:

- Monster, a job portal was hacked and private information of more than 1.3 million people were stolen in 2007 [2].
- FlexiScale is a provider for cloud service; an engineer suddenly deleted one of the main storage volumes. Processing services were unreachable until recovering of lost data was completed [3].

Received (May 25, 2017), Review Result (August 28, 2017), Accepted (September 1, 2017)
* Corresponding Author

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2017 SERSC Australia

- An indexing system at Zoho provided that one user could be able to read other users' documents through an unknown way [4].
- A tax collector offensively reached hundreds of private tax archive [5].

These cases, obviously show the necessity for accessing control policies. Regarding to these examples, data protection is necessary and protection of these data resources includes integrity, availability and confidentiality of information and services which are frequently stated and published as the CIA triad. Standardization is important in this area for security since the quality provided by these standards, interoperability, products and services efficiency can only be assured by utilization of standards. There is no comprehensive standard which can cover all the security aspects; among them is X.800 Recommendation [6]. Security services are categorized into five categories according to X.800 which are authentication (provides confirmation by using information such as user name-password), access control (protection against illegal usage of resources), data confidentiality (protection against unauthorized disclosure of information), data integrity (protection against unauthorized alteration of information) and non-repudiation (protection against refutation of one entities included in a communication) [7].

The cloud computing term, which is related to the new model for provisioning of computing infrastructure is still inadequately defined and understood, and is often described as a recreation of grid computing [8]. Therefore, the present definition of cloud computing focuses on an intensive provisioning of computational resources to various remote clients. Based on a research published in [9], Vaquero *et al*, proposed a definition for cloud computing: "Clouds are a large pools of easily practical and reachable virtualized resources (such as hardware, services)" [9]. These resources dynamically can be reconfigured to correct a variable load (scale), which also can lead an optimum utilization of resource. This pool of resources is usually exploited by a "pay-per-use model" in which guarantees are presented by the Infrastructure of customized SLAs.

This model became popular in business as a way for decreasing the upfront infrastructure investments, preservation costs and eventual replacement costs [8, 10].

In the present study at first we mention the significance of data security in cloud computing, then we review the architectural framework of cloud computing. After reviewing the literature about solutions of security, we will analyze the trust in cloud computing and finally we will review the security solutions.

2. Safety Challenges in Cloud Computing

Cloud system is different from the traditional system in the computer and can create new special security problems. The biggest concerns about cloud computing are security and privacy [11]. The following are some concerns beyond.

2.1. Network Availability

If the cloud is not available, the situation was no different with not services.

2.2. Management Access to Servers and Applications

One of the key characteristics of cloud computing is that "providers" access to the server computing, the Internet offers. In traditional data centers, manage access to the server, direct contact is limited. In the Cloud computing, the access management is now done through the Internet, which increases exposure the risk. To restrict access management and governance, protect critical changes in the control system [12].

 Copyright ⓒ 2017 SERSC Australia

2.3. Survival Cloud Provider

Because cloud providers are new to the marketplace, there are concerns about their commitment and survival this deeper concern is that when these providers need access to proprietary interfaces tenants that creates problems for tenants.

2.4. Dynamic Virtual Machines (Virtual Machine Mode Dispersion)

Virtual machines are used in dynamic cloud computing. They can quickly return to previous cases, stop and re-launched. They can also be easily cloned and transferred seamlessly between physical servers are the dynamic nature and potential for virtual machine sprawl makes it difficult to maintain a consistent security. Vulnerabilities or configuration errors may be unknowingly reproducing. Also, keep a record of an audit of the security situation virtual machine at any given point in time is difficult. In the cloud computing environment, will need to state security System, regardless of location or proximity to other proven and virtual machines to identify potentially unsafe.

2.5. Exploits of Vulnerabilities and Attacks VM-TO-VM

Server cloud computing operating systems and Web applications as virtual machines locally and physical servers they use. To lay the groundwork for an attack or malicious remote virtual cloud computing is a significant threat to the environment. In addition, the common place in several virtual machines at risk of attack VM-TO-VM increases.

2.6. Security Dormant Virtual Machines

Unlike a physical device, when a virtual machine is offline, still available to any program Which can store virtual machines on the network have it, and so prone to malware. However, VM dormant or offline, do not have the ability to run malware. Dormant virtual machines in just a hypervisor There may also be supported by other servers or storage media or archive. In the environment cloud computing responsibility to protect and scanning of dormant machines rests with the cloud provider. Companies using calculations Overcast need for cloud service providers that can secure and maintain the security of dormant virtual machines in the cloud Provide.

3. Security Strategies in Cloud Computing

Some security solutions to reduce security risks in cloud computing is discussed below.

3.1. Find the Best Cloud Provider

The first solution is to find the right cloud provider. There are various vendors to provide cloud. A seller Cloud should be well-established, experienced and implement standards and regulations [13].

For a cloud security standard should include the following:

- ✓ Access Control: This item should Implementation Guide and physical access to facilities and logical access to systems and Applications are.
- ✓ Disaster Response and its management should include details of all roles and responsibilities of the various parties associated with the table when it is, when an incident occurs.
- ✓ Backup system and network settings: It is very important that a valid copy or backup of all the settings your Including infrastructure components, servers, switches and host systems to be taken.

Copyright ⓒ 2017 SERSC Australia

- ✓ Test Security: The cloud provider should document the results of initial and periodic security testing to do.
- ✓ Encrypted data and communications: Standard must detail the functional areas (*e.g.*, web server traffic) and algorithms have approved encryption.
- ✓ Standard Password: The password quality standard acceptable to details, the parties must comply with (the especially during and train) are met.
- ✓ Continuous monitoring: It should detail how configuration management and change control to support the ongoing security in the country.

3.2. Data Recovery

Cloud vendors should provide very good facilities improvement. So, if the data is fragmented or because of some issues they have lost their cloud vendors can retrieve them.

3.3. Encryption

The main methods to ensure data security is in the cloud using encryption. Encryption seems to be the perfect solution to ensure data security is, however, not without difficulty [14]

3.4. Crushing Data

Some methods have been developed that can be used as alternatives to encryption. These encryption methods are generally faster than the bugs themselves. Splitting the data initially presented by Divyakant Agrawal and his colleagues. The idea is that information between divided into different host that the host can communicate with each other and only the owner can host access and combine data collected. This method is much faster compared to encryption but need to at least two independent service provider, but is homogeneous.

3.5. Using a Cloud Database (MCDB)

This method uses the split data in multiple cloud data across clouds are divided in a manner that Data confidentiality, integrity, and ensure the availability to maintain. Multi-cloud database storage model database Data in the cloud provides. MCDB single cloud model eliminates the negative effects and reduce security risks Brings. The destruction of a cloud, the information does not disappear [15].

4. Security Algorithms in Cloud Computing

In order to increase security in cloud computing, security models are used which some of them are mentioned below.

4.1. Defense in Depth

Defense in depth, a layer of protection model for important components of information systems. The strategy of defense in depth. The followings are included [16]:

- ✓ Network and infrastructure protection
- ✓ protection and defense in border areas (contact point network with other networks)
- ✓ The protection of the computing environment and operational
- ✓ Supporting infrastructure

 Copyright ⓒ 2017 SERSC Australia

4.2. Honeypots

Honeypot is a source of information system with false information against hackers and discovery and gathering activities. Unauthorized computer networks are on the network. Honeypot on computers that have the means to compromise computers that are either real or simulated have become.

So new tools and tactics can help hackers to attack systems record. Honeypots are Complex algorithms are very simple because they want to develop their state tables that need to be supported. The system administrator can see the techniques and methods used by the attacker to know how the system is broken and the vulnerability of the system to detect and act to repair Hani Patha. In short we can say that for two reasons used:

- ✓ system weaknesses
- ✓ Collecting information required to pursue and track hackers

4.3. Sandbox

When you surf a website and address in the URL you type in a web apparently site looks, but potentially, could have unintended threats to bring you the HTML code which is embedded. In this situation, the need for a protective indispensable for us and this is a "sandbox".

This is a preventive tool that puts the browser in a virtual environment as a result of any downloading programs malware via browser can affect your computer, it will prevent. Programs Applications that run in that environment, limited access to systems and various system files, hence the sandbox is a relatively thick layer protocol provides security. Sandboxing entrusted code and programs to carefully review and monitor the reduced attack surface. The operation of applications is blocked. Any code or programs the origin of the group of third-party suppliers, websites or users has not been approved to run by Sandbox are approved.

This feature, your Web browser is limited to a virtual environment and threats to computer programs the longer you use their influence to make it different. As a result, prevented malicious code from entering the OS Are. Sandbox for any unauthorized activity that should be performed by a program, or a program is run contrary to the nature of the block.

5. Importance of Security in Cloud Computing

Cloud Resources presented as a service based on your needs. Clouds may be generally a large number of commodity-grade servers, reliable service on demand and exploit deliver highly scalable. has increased the number of resources available in the network cloud to users as they need more resources and a reduction because they require less resources. These resources can be viewed as computer storage and other decisions. Cloud computing is noted as significant changes in the industry and more effectively address the development of information technology in society [17]. Including most of the infrastructure cloud computing services generally believed to be sent by data centers that have been established to a server with different levels of virtualization technologies. The service is available anywhere in the world, and the clouds come as a single point of access to all the needs of computer users. This technique changes the cloud computing software. Data stored in the cloud and users can be used anywhere at any time. This data is typically stored in a private system like a PC. Can guarantee the security of cloud computing and user data will be protected by him/herself. So cloud computing must guarantee the security of data stored in the cloud. Many companies offer cloud computing platforms like Google, IBM, Microsoft, Amazon, VMware and EMC [18-24].

Although cloud computing systems such as personal user data and personal data must be stolen, destroyed or removed. Since details are stored in the cloud system is necessary

Copyright ⓒ 2017 SERSC Australia

and important to users, hackers will have to pay more efforts to achieve the data. This system must be protected more than the traditional system. companies or consumers using the cloud system and the data stored in it. The data can also be viewed by any person that he / she is the person who is. If the insurance company in the cloud if they really need to store their personal data in the system. There are two key requirements for cloud governance and security, firewalls in the system or not. The problem is that most computer security can develop. This system cannot protect the cloud by traditional security mechanisms. The implementation of any cloud computing and mobility limitations and can create a lot of new security problems. Cloud computing is the most different problems, such as: data security, data privacy protection of users, cloud computing platform stability and administer cloud [17].

Security is one of the main obstacles and fears that hinder the widespread adoption of cloud computing [25]. Many industries, businesses and research organizations willing to set up depending on the clouds moving towards digital treasure third party service providers [26]. IT infrastructure can be traditional to digital asset holding companies or organizations the administrative domain. All processing, advanced, and data or execute applications in the management of the administrative domain. Instead, the organization does not want to control cloud services and infrastructure administration [27]. Safety procedures for (CSP) to the organization in general. The number of users is not an organization or company, exacerbate this concern [28]. If power to the consumer cloud service providers, but they cannot trust themselves or others. The reasons stated in the possession of the suspects and customers concerned about their digital resources located in the cloud comes from hate to embrace cloud computing [28].

Here we bring the study of literature on the issues of security of cloud computing. In [29, 30] the authors present the study because of security issues. Studies in the literature is limited only to the issues of safety and security solutions are not present. In [30] The authors review the security issues at different levels of cloud computing. Security solutions are presented in [30]. However, Abbas and Khan [30] said, a comprehensive study on the protection of privacy in the cloud with a focus on eHealth cloud. More than ever, this study is limited to privacy. In [31] The authors examine the challenges of security and privacy in cloud computing and discuss the defense strategy. The study was targeted because of security issues of privacy, integrity, accessibility, accountability, and privacy preservability there is little information about the technology leads to a fundamental weakness [31]. Neng *et al* (2013) have described the security issues cloud the approach to address vulnerability [32]. On the other hand, is not a study about the direction of future research are presented in the literature. Similarly, the research mentioned in computing security issues [33] cloud detailed summary of the discussions about the present and the latest solutions. Che *et al* (2011) studied the security model of cloud computing adoption, such as the cube model, a rental model, and a risk assessment model [34]. Furthermore, they called on the security risks of cloud computing. So the risk of side various stack holders', such as customers, governments, and service providers to discuss. No safety issues were submitted for study and practical technology perspective. Also, there are strategies to mitigate the security issues that were examined as the term "any component and make sure the process and should be considered". Also, reference [35] described the security issues of cloud computing and their solutions. So the investigation was focused more on the privacy of cloud security. Furthermore, there is no paper on the direction of future research.

6. Architectural Framework

Cloud computing integrates a variety of computing techniques to afford services for the users. Definition of National Institute of Standards and Technology’s (NIST) is commonly accepted [25, 38]. This definition considers the cloud computing as a threefold

 Copyright ⓒ 2017 SERSC Australia

service provisioning model, consists of: essential specifications, service models, and operation models [36]. According to this definition the main concept of cloud computing is presented in tables 1-3.

Table1. Essential Characteristics of Cloud Computing Architecture [25]

service	Concept
On-demand self-service	Request and manage the service from the cloud without any human interaction with CSP
Broad network access	By using from standard mechanisms and protocols, service and data present on the cloud
Resource pooling	Resources are shared among customers by pooling in a multi-tenant environment

Table 2. Service Models of Cloud Computing Architecture [25]

service	Concept
SasS [32]	Enables the customers to use CSP's applications, running on the cloud infrastructure, through the Internet
PaaS [31]	Owned by the customer requirement a framework where they can be executed and managed
IaaS [29]	Hardware infrastructure provided by the CSP including the network, storage, memory, processor, and various other computing resources

Table 3. Deployment Models of Cloud Computing Architecture [25].

service	concept
Private Cloud	Run and managed only for a single organization
Public Cloud	Physical infrastructure is owned by the CSP and is open to general public and organizations
Community cloud	Shared by a number of organizations and/or customers forming a community

7. Cloud Computing Security Solutions

Regarding to the structure of multiuser and resource sharing, there are several requirements for cloud computing security. The following models are extracted from literature and are some practical solution for cloud computing security.

7.1. Security Access Control Service (SACS)

Jing, and Jian-Jun, in their study proposed a technological solution. Modified services are the cloud computing service delivery basis [33]. These services are supported by the resource and upper layer services which require some security determination to guarantee that only the proper person will be able to use safely by having availability to this environment [33-34]. Combination of Access Authorization, Programming Interface Security Application (Security API), and security of cloud connection with the presented architecture of cloud computing, is located at the bottom of the tested approach which is referred as SACS model [33]. The advantage of this model is the authentication and available controlling through certification and derivable service resources list. This model is indicated in Figure 1 [33] as the following:

Copyright ⓒ 2017 SERSC Australia

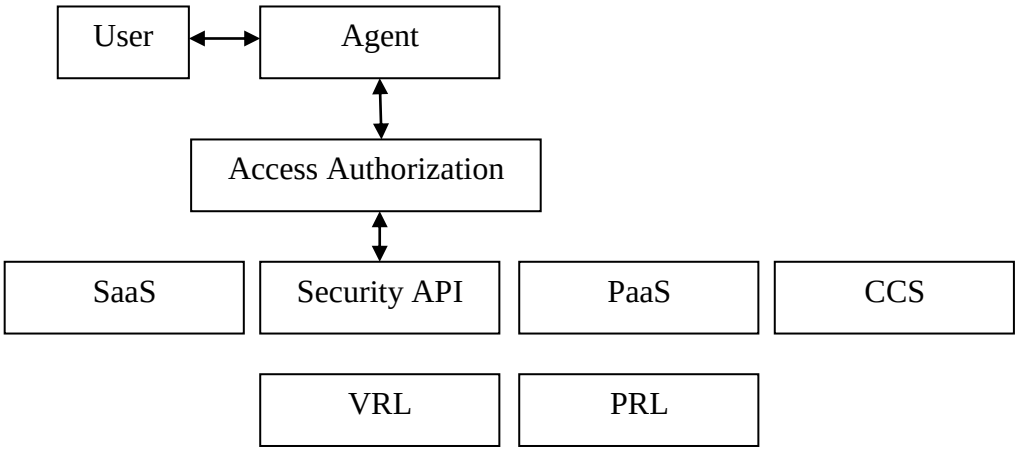

Figure 1. Cloud Computing Security Model [33]

7.2. Fully Homomorphic Encryption

Homomorphic encryption code is defined as "especial type of calculation allows to do it and the result is encrypted cipher text corresponding to the results of operations performed on text to create" [38]. This is a good trait in a modern communications system architecture. Homomorphic encoding and encryption can be responsible for various services that chaining together without disclosing the details of each one. Cloud computing can provide computing capacity, data and information that is encoded and stored in the cloud, but if a user can use cloud features, such as computing power, CSP should hold the key. The main idea of this encryption technology model under mirroring the [37-38]. Therefore, the main problem with using the same public key for encoding data. So share information impossible.

7.3. Trusted Computing Platform

Web services standard instruments and software security model of most cloud computing today primarily because of the conduct and management of sponsored messages. This model has some drawbacks, such as: the lacks of hardware is not adequately secure and protect the construction certificate. Will achieve security for the data in its primary role of the Trusted Computing (TC), instead of using add-on applications [37, 39]. Shen and Tong [39] said the Trusted Computing Platform (TCP) for authentication and encryption coding. Can According to their study of the benefits of the model as follows: from the computer's CPU power, better hardware integration of the main private users. But in addition to hardware requirements cost disadvantage of this model.

7.4. Storage Security in Cloud Computing

Rajathi, and Saravanan in their study [40] mentioned the advantages of several offered computing storage frameworks and technologies cloud. The main techniques of this scheme are summarized in table 4. According to [40-41], the aim of this technique is achieving appropriate security and data accessibility by usage of Token generation algorithm with homomorphic token and integration algorithm [40-41].

 Copyright ⓒ 2017 SERSC Australia

Table 4. Advantages and Limitations of the Mentioned Model [40]

Storage	advantages	limitation
embedded Storage Security to Online data	Partitioned data pieces cannot bring out any user information. In case user forgot where the data stored	it will become difficult for users.
Identity-Based Authentication	Weightless and more expeditious	Only certificate communication is taken into account
Public Auditing with Complete Data Dynamics support	Basic Markle Hash Tree (MHT) is manipulated for block tag authentication.	Computation cost of BLS scheme is prominent
Efficient Third Party Auditing (TPA)	Auditor performs auditing jobs for different users at the same.	Unable to support both public verification and dynamic data correctness
Way of Dynamically Storing Data in Cloud	Integrity can be verified before and after data insertion.	TPA is not considered for integrity checking process.
Effective and Secure Storage Protocol	Block level data dynamic operations are also used to maintain the same security assurance	Elliptic Curve Cryptography scheme is only suitable for devices with restricted low power
Storage Security of Data	Provided data backups for data recovery. Includes essential security services such as authentication, encryption and decryption and compression	Data backups are available at multiple servers. So there is a chance for servers to behave unreliably.
Secure and Dependable Storage Services	Guaranteed the correctness insurance and also identified immoral server behavior. Gross overhead approximately stays equal with other	Guaranteed the correctness insurance and also identified immoral server behavior. Gross overhead approximately stays equal with other
Optimal Cloud Storage Systems	Proposed generic architecture served as blueprint for optimal storage controller. Need to integrate with frontends for future research	Proposed generic architecture served as blueprint for optimal storage controller. Need to integrate with frontends for future research
Process of access and Store Small Files with Storage	Improves the access ability of small files. Cutoff point is measured to improve I/O performance. Formula for cut	off point not available
File Storage Security Maintenance	File chunking operation is carried out to provide data backups in case of server failure. Data chunks are stored in slave server will lead to an opportunity of corrupting data by servers	File chunking operation is carried out to provide data backups in case of server failure. Data chunks are stored in slave server will lead to an opportunity of corrupting data by servers

8. Security Solutions

Measures to address the issues of communication and networking to ensure relevant, CSA guidelines [42] recommend using a combination of virtual local area network, IDS, IPS, and firewall to protect data in transit. Instructions leakage of customer information about virtual network using the same basic infrastructure focus. CSA recommends the use of tools with strict access management policies. The use of virtual machines and physical machines with standard hypervisor with sticky absorbed by CSA certified vision and monitoring traffic on the virtual network. advanced cloud protection system (ACPs) in [41] that aims to provide security for the cloud resources. ACP countries and CSP

Copyright ⓒ 2017 SERSC Australia

including network resources to users and data to a wide range of security services provider CSP.

In addition, ACP countries can also bring the ability to review the actions of the virtual machine. ACP countries are divided into different modules located on the host platform. Interceptor modules has led to the discovery of any suspicious activity in the host. suspicious activity is detected by a recording that is stored in our comics warning module. As security threats, security policy rate increase female sex careful handling module actuators for active treatment. Czech ACPs Sam calculate critical infrastructure including network installation time. Full control of the computer infrastructure objects studied by evaluating asynchronous. volume control continues approved under constant supervision to clear the entrance. To prevent attacks on the network infrastructure, the ACP countries to use the method proposed in [43] where the search network using IP identification and alert warnings listed in the table pool. In addition to network security and other critical infrastructure that provides ACP countries to provide security against malicious attacks and VMS data. One of the main features of the countries which still ACP transparent to the virtual machine and cannot be detected. Interceptor module does not prevent any responses to prevent your system identified. However, the task is taken strike after it is approved. Calls will be allowed to stop the attack in the early detection of any surveillance system. ACP countries prototype in Eucalyptus open source cloud and ECP Open the system was implemented. safety devices for cloud computing, called Cyber Guarder. In [44], cyber security through the use of virtual networks provides a secure system.

In addition, the remote virtual network using Layer Two Tunneling Virtual Private Network (VPN) between the virtual bridge was introduced [45]. Data between virtual machines on the method of peer-to-peer (P2P) without transit passes through a central server. However, the metadata in the central node for traffic between VMMs optimized storage. port software designed to monitor network traffic. Typical security web systems such as security intrusion detection system (IDS) virtual network adapter for applications running in virtual network that will be used. In addition, VM CyberGuarder safety by monitoring the integrity of the application and provides system calls used by applications. The experimental results show that due Cyberguarder and 5% to 10% performance increase in energy consumption overhead.

Wu *et al* [45] to develop a virtual network virtual network protection against sniffing and spoofing attacks available. The Xen hypervisor is used to indicate the time. Utility models planned between the bridge and the road Xen hypervisor for virtual network configuration. The Bridge connects directly Xen VM virtual Ethernet bridge. The bridge is also connected to the physical network. P2P connection road between the VM and the range of 0 (management VM) creates. (A) routing, (b) firewall, and (c) the shared network layer: three-tier model, divided. Creating a logical channel specific set of routing between virtual and physical networks. Each channel has a unique identifier is reasonable to monitor the closed-source coming from the network. Firewall set for protection against spoofing attacks shared network. This series ensures that each virtual interface connected to a virtual network that is shared with any other virtual network is not communicating. Monitored by the logical identifier assigned by the routing layer. In the second stage, a layer firewall to allow the package to update routing tables. All packets are discarded. network layer connection shared between virtual machines, virtual networks associated with different channels at all.

XHe *et al*, deliver cloud solutions in web security [45] as a novel solution through basic firewall rules. The researchers showed that the traditional firewall rules vulnerable to security issues shadow government, sewers position, and the rest of the law. Moreover, firewall rules after the regulations referred less search function decline because of successive governments and the rules of the older ones. To eliminate these problems, the authors firewall rule is that laws Tree list is presented in a tree instead. Features of the

 Copyright ⓒ 2017 SERSC Australia

design compared to the first packet header matching node tree roots and results to the next level tree nodes.

9. Conclusion

In this study, we tried to review the security challenges in the cloud system. Cloud computing have been brought rapid development and shows excellent scenario and great potential. The cloud computing can be related to many areas of information management and services. The data security and privacy issue in cloud environment is more important rather than the usual network because the information in cloud computing environment is significantly related to the network and server. In this regard these problems had been caught up the enhancement in cloud computing area and also security affairs are considered as the main problem. CCPs should create lots of evaluation in order of efficient protection from security for problems solving.

References

[1]. F.G. George, "National information systems security (INFOSEC) glossary", Meade, Md.: National Security Agency, **(1997)**.
[2]. A. Sezen, "Cloud computing security issues and selection of deployment model and service model according to security requirements", Ms.C thesis, ATILIM UNIVERSITY, **(2015)**.
[3]. S. A. Ahson and M. Ilyas, "Cloud Computing and Software Services Theory and Techniques", CRC Press, **(2011)**.
[4]. S. Mansfield-Devine, "Cloud Security: Danger in the clouds", vol. 2008, no. 12, **(2008)**, pp. 9-11.
[5]. X. Recommendation 800, "In Security architecture for open systems interconnection for CCITT application", Geneva, **(1991)**.
[6]. W. Stallings, "Cryptography and Network Security: Principles and Practice", 5th ed., Marcia Horton, Ed. New York, America: Prentice Hall, **(2011)**.
[7]. L. M. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner, "A break in the clouds: towards a cloud definition", SIGCOMM Comput. Commun. Rev., vol. 39, **(2008)**, pp. 50–55.
[8]. B. Sotomayor, R. S. Montero, I. M. Llorente and I. Foster, "Virtual infrastructure management in private and hybrid clouds", IEEE Internet Computing, vol. 13, **(2009)**, pp. 14–22.
[9]. P. Mell and T. Gance, "The nist definition of cloud computing", tech. rep., National Institute of Standards and Technology, **(2011)**.
[10]. "A Trend Micro White Paper", Making Virtual Machines Cloud-Ready, **(2010)**.
[11]. P. K. Tiwari and B. Mishra, "Cloud Computing Security Issues, Challenges and Solution", International Journal of Emerging Technology and Advanced Engineering, **(2012)**.
[12]. J. Weis and Alves-Foss, "Securing Database as a Service", IEEE Security and Privacy, **(2011)**.
[13]. B. Meine, "book cloud computer security techniques and tactics", **(2011)**.
[14]. M. AlZain, B. Soh and Pardede, "A New Approach Using Redundancy Technique to Improve Security in Cloud Computing", IEEE, **(2012)**.
[15]. B. S. Kaliski, Jr. and W. Pauley, "Toward risk assessment as a service in cloud environments", Proceedings of the 2nd USENIX conference on Hot topics in cloud computing (HotCloud'10), USENIX Association, Berkeley, CA, USA, pp.2013
[16]. W Liu, "Research on Cloud Computing Security Problem and Strategy", IEEE journal of cloud computing, 978-1-4577-1415-3, **(2012)**.
[17]. P. Pandey, P. Dhasal and R. Pandit, "Trusted Security Model for User's Data for Public Cloud Using RSA Encryptio", International Journal of Emerging Technology and Advanced Engineering, **(2014)**.
[18]. S. Singh, "Data Security Issues and Strategy on Cloud Computing", IJSETR, vol 2, no. I 8, **(2013)**.
[19]. W. Liu, "Research on Cloud Computing Security Problem and Strategy", 978-1-4577-1415-3/12, IEEE, **(2012)**.
[20]. J. Sen, "Security and Security and Privacy Privacy Privacy Issues in Cloud Computing Computing", Tata Consultancy Services Ltd., Kolkata, INDIA, **(2009)**.
[21]. SAN Virtuosity Series, "VMware vSphere Data Protection and Security Compliance forCisco/Emulex SANs", vmware, **(2010)**.
[22]. B. J. Dooley, "Blue Clouds on the Horizon—IBM Designs for the Stratosphere", Navigating Information Technology Horizons, **(2008)**.
[23]. C. Vázquez Blanco and B. Sotomayor, "OpenNebula Tutorial", Distributed Systems Architecture Research Group Universidad Complutense de Madrid, **(2010)**.
[24]. D. AB. Fernandes, L. FB. Soares, J.V. Gomes, M.M. Freire and P. RM Inácio, "Security issues in cloud environments: a survey", Int. J. Inform. Sec., vol. 13, no. 2, **(2014)**, pp. 113–170.

Copyright ⓒ 2017 SERSC Australia

[25]. R. Latif, H. Abbas, S. Assar and Q. Ali, "Cloud computing risk assessment: a systematic literature review", in: Future Information Technology, Springer, Berlin, Heidelberg, **(2014)**, pp. 285–295.
[26]. A.N. Khan, M.L.M. Kiah, M. Ali, S.A. Madani and S. Shamshirband, "BSS: block-based sharing scheme for secure data storage services in mobile cloud environment", J. Supercomput., vol. 70, no. 2, **(2014)**, pp. 946–976.
[27]. R. Latif, H. Abbas, S. Assar and Q. Ali, "Cloud computing risk assessment: a systematic literature review", in: Future Information Technology, Springer, Berlin, Heidelberg, **(2014)**, pp. 285–295.
[28]. C. Rong, S.T. Nguyen and M.G. Jaatun, "Beyond lightning: a survey on security challenges in cloud computing", Comput. Electr. Eng., vol. 39, no. 1, **(2013)**, pp. 47–54.
[29]. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", J. Netw. Comput. Appl., vol. 34, no. 1, **(2011)**, pp. 1–11.
[30]. C. Modi, D. Patel, B. Borisaniya, A. Patel and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing", J. Supercomput., vol. 63, no. 2, **(2013)**, pp. 561–592.
[31]. Y. Neng-Hai, Z. Hao, J. Xu, W. Zhang and C. Zhang, "Review of cloud computing security", Acta Electron. Sinica, vol. 41, no. 2, **(2013)**, pp.371–381.
[32]. K. Hashizume, D.G. Rosado, E. Fernndez-Medina and E.B. Fernandez, "An analysis of security issues for cloud computing", J. Internet Services Appl., vol. 4, no. 1, **(2013)**, pp. 1–13.
[33]. J. Che, Y. Duan, T. Zhang and J. Fan, "Study on the security models and strategies of cloud computing", Proc. Eng., vol. 23, **(2011)**, pp. 586–593.
[34]. Z. Tari, "Security and privacy in cloud computing", IEEE Cloud Comput., vol. 1, no. 1, **(2014)**, pp. 54–57.
[35]. P. Mell and T. Grance, "The NIST definition of cloud computing (draft)", NIST Special Publ., vol. 800, no. 145, **(2011)**, p. 7.
[36]. K. Hashizume, D.G. Rosado, E. Fernndez-Medina and E.B. Fernandez, "An analysis of security issues for cloud computing", J. Internet Services Appl., vol. 4, no. 1, **(2013)**, pp. 1–13.
[37]. P. Mayer, "Data Recovery: Choosing the Right Technologies", datalink, **(2003)**.
[38]. Z. Shen, and Q. Tong, "The security of cloud computing system enabled by trusted computing technology", in Proc. ICSPS'10, **(2010)**, p. V2-11-V2-15.
[39]. J. Feng, Y. Chen, D. Summerville, W-S Ku and Z. Su, "Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol", in Proc. IEEE CCNC'11, **(2011)**, p. 521-522.
[40]. P. M. Deshmukh and A. S. Gughane, "Maintaining File Storage Security in Cloud Computing", International Journal of Emerging Technology and Advanced Engineering, vol. 2, no. 10, **(2012)**, pp. 2250-2459.
[41]. C. Wang, Q. Wang, K. R. Wenjing and W. Lou, "Ensuring Data Storage Security in Cloud Computing", Quality of Service, **(2009)**.
[42]. F. Lombardi and R.D. Pietro, "Secure virtualization for cloud computing", J. Netw. Comput. Appl., vol. 34, no. 4, **(2011)**, pp. 1113–1122.
[43]. Cloud security alliance, "security guidelines for critical areas of focus in cloud computing v3.0", **(2011)**.
[44]. T. Ristenpart, E. Tromer, H. Shacham and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", in: Proceedings of the 16th ACM Conference on Computer and Communications Security, **(2009)**, pp. 199–212.
[45]. H. Wu, Y. Ding, C. Winer and L. Yao, "Network security for virtual machine in cloud computing", in: 5th International Conference on Computer Sciences and Convergence Information Technology, **(2010)**, pp. 18–21.

Authors

Fatemeh Sedaghat, she received her B.Sc. degree in computer hardware engineering. She is currently a MSc. Student in Computer Engineering Department, Yadegar-e-Imam Khomeini (RAH) Shahre Rey Branch, IAU University, Tehran, Iran. She has been engaged in research in the field of cloud computing and wireless sensor networks.

 Copyright ⓒ 2017 SERSC Australia

Majid Haghparast, he received his B.Sc. in computer hardware engineering in 2003. He received his M.Sc. and Ph.D. degrees in computer architecture in 2006 and 2009, respectively. Since 2007, he has been affiliated with the Computer Engineering Faculty, Yadegar-e-Imam Khomeini (RAH) Shahre Rey Branch, IAU University, Tehran, Iran. His research interests include computer arithmetic and reversible logic circuits. Since April 2017 he is conducting his sabbatical at the Johannes Kepler University Linz, Austria, where he also is a Research Fellow. Dr. Haghparast is on the panel of reviewers for various international journals.

Mehrdad Maeen, he received his B.Sc. in Computer Engineering from faculty of electrical and computer engineering of Shahid Beheshti University in 2007 and the M.Sc. and Ph.D. degrees from the Tehran Science and Research Branch of Islamic Azad University. Currently, he is an Assistant Professor of the Computer Engineering Faculty, Yadegar-e-Imam Khomeini (RAH) Shahre Rey Branch, IAU University, Tehran, Iran. His research interests include modeling and design of low-power VLSI circuits and computer arithmetic.

Copyright ⓒ 2017 SERSC Australia

Copyright ⓒ 2017 SERSC Australia