Scientific Research Publishing

Journal of Computer and Communications, 2021, 9, 31-42
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Multilayer Security Framework for Cloud Computing in Internet of Things (IoT) Domain

M. Mamun-Ibn-Abdullah, M. Humayun Kabir*

Department of Electrical and Electronic Engineering, Islamic University, Kushtia, Bangladesh
Email: *humayun@eee.iu.ac.bd

How to cite this paper: Mamun-Ibn-Abdullah, M. and Kabir, M.H. (2021) A Multilayer Security Framework for Cloud Computing in Internet of Things (IoT) Domain. *Journal of Computer and Communications*, **9**, 31-42.
https://doi.org/10.4236/jcc.2021.97004

Received: June 26, 2021
Accepted: July 24, 2021
Published: July 27, 2021

Abstract

Cloud computing is a type of emerging computing technology that relies on shared computing resources rather than having local servers or personal devices to handle applications. It is an emerging technology that provides services over the internet: Utilizing the online services of different software. Many works have been carried out and various security frameworks relating to the security issues of cloud computing have been proposed in numerous ways. But they do not propose a quantitative approach to analyze and evaluate privacy and security in cloud computing systems. In this research, we try to introduce top security concerns of cloud computing systems, analyze the threats and propose some countermeasures for them. We use a quantitative security risk assessment model to present a multilayer security framework for the solution of the security threats of cloud computing systems. For evaluating the performance of the proposed security framework we have utilized an Own-Cloud platform using a 64-bit quad-core processor based embedded system. Own-Cloud platform is quite literally as any analytics, machine learning algorithms or signal processing techniques can be implemented using the vast variety of Python libraries built for those purposes. In addition, we have proposed two algorithms, which have been deployed in the Own-Cloud for mitigating the attacks and threats to cloud-like reply attacks, DoS/DDoS, back door attacks, Zombie, etc. Moreover, unbalanced RSA based encryption is used to reduce the risk of authentication and authorization. This framework is able to mitigate the targeted attacks satisfactorily.

Keywords

Cloud Computing, Data Security, Embedded Platform, Framework, Security Threat

1. Introduction

Cloud computing is considered as a blessing of modern technology which has

made a revolutionary change in our thinking about storing data. It is a low-cost and remotely accessible system. We can store a huge amount of data and access it from anywhere in the world at any time. In few years Cloud computing has grown up from just being a concept to one of the major part of IT industry. It is widely accepted as the adoption of virtualization, SOA and utility computing. Cloud computing defines as a paradigm for enabling useful, on-demand network access to a shared pool of configurable computing resources by The National Institute of Standard and Technology (NIST). It generally works on three types of architecture aspects namely SaaS (software as a service), PaaS (platform as a service) and IaaS (infrastructure as a service). Software as Service (SaaS) serves the services that exist in the cloud or applications to the end-users, whereas Platform as Service (PaaS) offers accessibility of the platforms and Infrastructure as Service (IaaS) provides processing, storage and other computing resources.

Cloud computing has various advantages and its application has drastically increased in today's IT based modern life. Due to its enormous benefits more and more individuals and companies are placing their important information in the cloud and therefore concerns are rising especially about the security of the data stored in the cloud. Protecting data from unauthorized or third-party authenticator is our main objective. The externalization of users, making it hard to maintain data integrity, availability and privacy, that causes serious consequences. Ensuring the security of cloud is one of the biggest challenges in cloud computing systems [1] [2] [3]. In recent years, cloud services appear many security accidents. For example, in March 2009, Google leaked a large number of documents. Microsoft Azure platform stopped working for about 22 hours. In April 2011, Amazon's EC2 service disruptions, influences the service of Quora, Reddit, etc.

These security problems caused a devastating blow. Therefore, to make the enterprise and the organization accept cloud computing services, it is necessary to solve the security problems involving it [4] [5]. Because of the high security concerns, organizations are integrating various strategies and tools (like cloud management and monitoring tools, and cloud security management tools) to lessen these challenges. In this research, we discuss the possible threats\attacks present in cloud computing environment and we propose our security model and framework for mitigating all those security concerns in cloud computing environments.

This research is organized as follows: Section 2 introduces literature review. Section 3 includes an overview of cloud platform, Section 4 presents proposed security model and framework. Section 5 describes performance evaluation and finally, Section 6 concludes with mentioning future work.

2. Literature Review

Many researches had been performed a valued discussion about the security related issues in Cloud computing systems submitting a qualitative analysis and

surveys related to the security issues. They propose some security strategies to develop and deploy a qualitative security management framework on cloud computing systems. Kashif *et al.* proposed a security model and framework for secure cloud computing systems that identifies the security requirements, attacks, threats and concerns associated to the deployment of the clouds [6]. They also proposed that cloud security is not just a technical problem, but also involves standardization, supervising mode, laws and regulations, and many other aspects. Cloud computing is associated with development opportunities and challenges, along with the security problem must be solved step by step. Ukil *et al.* have analyzed security problems in cloud computing [7]. They proposed a framework satisfying cloud security ensuring the confidentiality, integrity and authentication of data. They provide security architecture and necessary security techniques for cloud computing infrastructure.

Hu *et al.* present a Law-as-a-Service (LaaS) model for automatic enforcing of legal policies to handle queries for cloud service providers (CSPs) and their customers [8]. The law-aware super-peer acts as a guardian providing data integration and protection. Sun *et al.* present a dynamic multidimensional trust model in the basis of time-variant comprehensive evaluation multi-dimensional method [9]. In [2] the authors proposed a generic security management framework allowing providers of cloud data management systems to define and enforce complex security policies. They designed the framework to detect and stop a large number of attacks defined through an expressive policy description language and to be easily interfaced with various data management systems. They showed that they can efficiently protect a data storage system by evaluating their security framework on top of the BlobSeer data management platform. The benefits of preventing a DoSattack targeted towards BlobSeer were evaluated through experiments performed on the Grid5000 test bed. The work in [3] investigated the problem of assuring the customer of the integrity (*i.e.* correctness) of his data in the cloud. The cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised since the data is physically not accessible to the user. The authors provided a scheme which gives proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. In [4] the author discussed some security and privacy issues in Cloud computing and suggested four methods for cloud security and privacy including Access control method, policy integration, identity management method and user control method.

In [10] the authors discussed the security issues in a Cloud computing environment. They focused on technical security issues arising from the usage of cloud services. They discussed security threats presented in the cloud such as VM-Level attacks, isolation failure, management interface compromise and compliance risks and their mitigation. In [11] the authors analyzed vulnerabilities and security risks specific to cloud computing systems. In [12] the author discussed some vital issues to ensure a secure cloud environment. This included a basic view of security policies (e.g., inside threats, access control and system

portability), software security (e.g., virtualization technology, host operating system, guest operating system and data encryption) and hardware security (e.g., backup, server location and firewall). The author concluded that an important issue for the future of cloud security is the use of open standards to avoid problems such as vendor lock-in and incompatibility.

La'Quata Sumter *et al.* [8] illustrate the rise in the scope of cloud computing has brought fear about Internet security and the threat of security in cloud computing is continuously increasing. In [9] Meiko Jensen has shown that in order to improve the security of cloud computing, the security capabilities of both web browsers and web service frameworks, should be strengthened. This can best be done by integrating the latter into the former. They focus on special type of Denial of Service attacks on network based service that relies on message flooding techniques, overloading the victims with invalid requests. They describe some well-known and some rather new attacks and discuss commonalities and approaches for countermeasures. Armbust M Fox *et al.* [12] discuss that resources should be virtualized to hide the implementation of how they are multiplexed and shared. Shaping the security of critical systems is very important. Addressing the security issues faced by end-users is extremely mandatory, Researchers and professionals must work on the security issues associated with cloud computing. Strong security policies must be designed to ensure data is safe and prevented from unauthorized access, in both corporate data centers and in the cloud servers. M. Okuhara *et al.* [13] explain how customers, despite their deep-seated concerns and uneasiness about cloud computing, can enjoy the benefits of the cloud without worry if cloud services providers use appropriate architectures for implementing security measures. They also describe the security problems that surround cloud computing and outline Fujitsu's security architecture for solving them. In [14] author discusses the fundamental trusted computing technologies on which latest approaches to cloud security are based. In [15] argues that, with continued research advances in trusted computing and computation supporting encryption, life in the cloud can be advantageous from a business-intelligence standpoint, over the isolated alternative that is more common nowadays.

Many researchers have proposed various security frameworks carried out relating to the security issues in cloud computing in numerous ways. However, they do not propose a quantitative approach to analyze and evaluate privacy and security in cloud computing systems. This research primarily aims to analyze and evaluate the most known cloud security problems in cloud computing systems and we focus on a few threats and attacks and try to mitigate these security problems by developing algorithms.

3. Overview of Cloud Computing

As with any new technology, the definition of cloud computing is changing with the evolution of technology and its services. No standard definition for cloud

computing has yet been agreed upon, especially since it encompasses so many different models and potential markets, depending on venders and services. In the simplest of terms, cloud computing is basically internet-based computing. The term "Cloud" is used as a metaphor for the Internet, and came from the well-known cloud drawing that was used in network diagrams to depict the Internet's underlying network infrastructure. The computation in the internet is done by groups of shared servers that provide on-demand hardware resources, data and software to devices connected to the net. The National Institute of Standards and Technology NIST, gives a more formal definition: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". NIST also notes that this definition will probably change over time. Cloud computing architecture has three main deployment models which are Private, Public and Hybrid Cloud. The services provided by Cloud computing can be categorized into three service models, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These three models often abbreviated as the SPI Service framework (*i.e.* SPI is short for Software, Platform and Infrastructure) are the basis of all services provided by Cloud computing.

3.1. Infrastructure-as-a-Service

IaaS service model is the lowest level of service provided to the client. In this service model, the Cloud computing client is provided with controlled access to the virtual infrastructure. Using this access, the client can install operating system and application software. From the client's point of view, this model is similar to renting the hardware from a service provider and letting the service provider manage the hardware. This model requires the client to have highly experienced network engineer(s). Handling everything from the operating system and up is a big responsibility that most clients decline to handle, especially because of the security burdens. Thus, this model is not of high preference in the Cloud computing client's society.

3.2. Platform-as-a-Service

In PaaS, the operating system and all platform-related tools (like compilers) are already installed for the client. These pre-installed components are also managed by the cloud service provider. Clients have the freedom of installing additional tools based on their needs. However, the control over the infrastructure is retained by the service provider. The client controls applications development, configuration, and deployment. The major difference between this model and traditional web hosting is rapid provisioning. Traditional web hosting is managed manually and requires human intervention when the demand increases or decreases. On the other hand, provisioning in Cloud computing is automatic

and rapid. Thus, it does not require any human interventions.

3.3. Software-as-a-Service

SaaS model focuses on the application level and abstracts the user away from infrastructure and platform details. Usually, applications are provisioned via thin client interfaces such as web browsers or even mobile phone apps. Microsoft's Outlook.com is a clear example of this. An organization can adopt Outlook.com electronic mail service and never bother with hardware maintenance, service uptime, security, or even operating system management. The client is given control over certain parameters in the software configuration, for example, creating and deleting mailboxes. These parameters can be controlled through the interface of the application.

Cloud computing's key security requirements coupled with Cloud computing deployment models and Cloud computing service delivery models and can be seen in context as a guideline to assess the security level. In Table 1 compulsory requirements are represented by the "√" symbol and optional requirements are represented by the "×" symbol.

4. Proposed Security Model and Framework

In this subsection, we describe security model for Cloud computing against threats mentioned in previous section, which focuses on scalability and security. The model is shown in Figure 1 and it consists following security units. Table 2 shows the list of threat which was addressed in this framwrok.

User can be certificated by the 3rd party certificate authority, then can be issued token for service by End User Service Portal. After joining service portal, user can purchase and use cloud services which are provided by single service provider. End User Service Portal which is composed access control, security policy, Key management, service configuration, auditing management, and virtual environments provides secure access control using Virtual Private Network (VPN) and cloud service managing and configuration.

Table 1. Key security requirements coupled with cloud computing deployment models and cloud computing service delivery models.

Cloud Deployment Models	Private/Community Cloud			Public Cloud			Hybrid Cloud		
Confidentiality	√	√	×	×	√	×	√	×	×
Integrity	√	√	×	√	×	√	√	√	√
Authentication	√	×	√	√	×	√	√	×	×
Availability	√	√	√	×	√	√	×	×	×
Accountability	√	×	×	√	√	√	√	×	×
Cloud Service Delivery Models	SaaS	Paas	IaaS	SaaS	Paas	IaaS	SaaS	Paas	IaaS

Table 2. List of threats which meet the proposed framework.

Threats and Attacks	Affected cloud services	Definition	Mitigation
Reply Attack	SaaS	An attacker can sniff the packet using another device connected to a computer and capture the packets transmitted. Attacker can replay the same packets, or even change the data contained in that packet that may causing an unaccepted behavior in the network.	**Algorithm 1** (This algorithm is explained in Chapter seven)
Identity Theft	IaaS, PaaS, SaaS	Occurs when an attacker pretends to be someone else to get users credentials.	Strong password, authentication and access control mechanisms. (Unbalanced RSA Algorithm)
Backdoor channel attack	SaaS	It is a detached attack, which enables programmers to increase remote access to the undermined framework. Utilizing backdoor channels, programmers can have the option to control unfortunate casualty's assets	**Algorithm 2** (This algorithm is explained in Chapter seven)
DOS/DDOS Attacks	Application Level	Attacker tries to make the services unavailable by launching SYN flooding, UDP flooding, and ICMP flooding attacks etc.	
Zombie Attacks	Network Level/VM Level	Victim's Virtual Machines (VMs) is flooded by means of sending requests from other VMs in the network.	

5. Evaluation of the Proposed Framework

For implementing the proposed security framework we have developed an Own-Cloud platform using a 64-bit quad-core processor based embedded system (Raspberry pi) where an external hard drive is used as the cloud storage. Raspberry pi based personal cloud server allows real time data transfer without any data rate limitation as user is the only one who can use it. The server is built based on a local sensor network, meaning that the Raspberry Pi and sensor node are on the same network. However, user can access his cloud server from anywhere outside the server network by a process called port forwarding. The size of the database depends largely on the size of the hard drive mounted on the Raspberry Pi. For this prototype we have used a 32 GB SD-card for cloud storage. However, for larger database, we can use portable hard disc of any size. Raspberry pi based Own-Cloud platform is quite literally as any analytics, machine

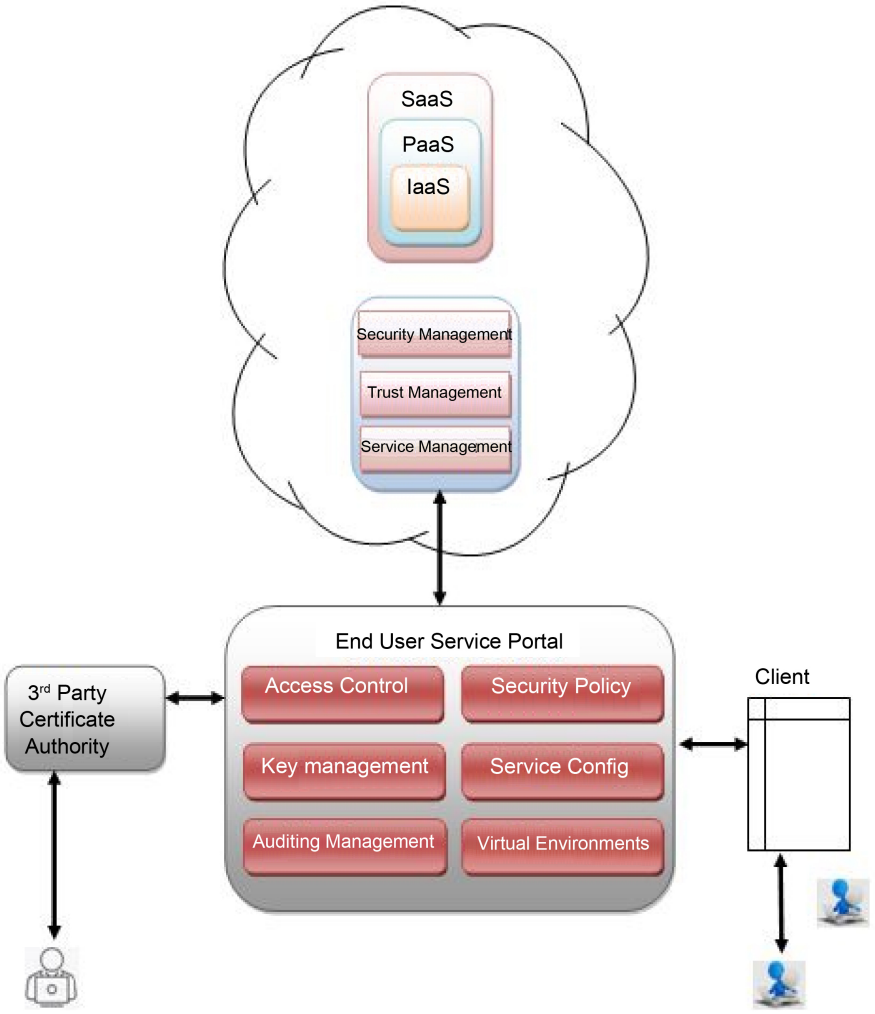

Figure 1. Proposed security model.

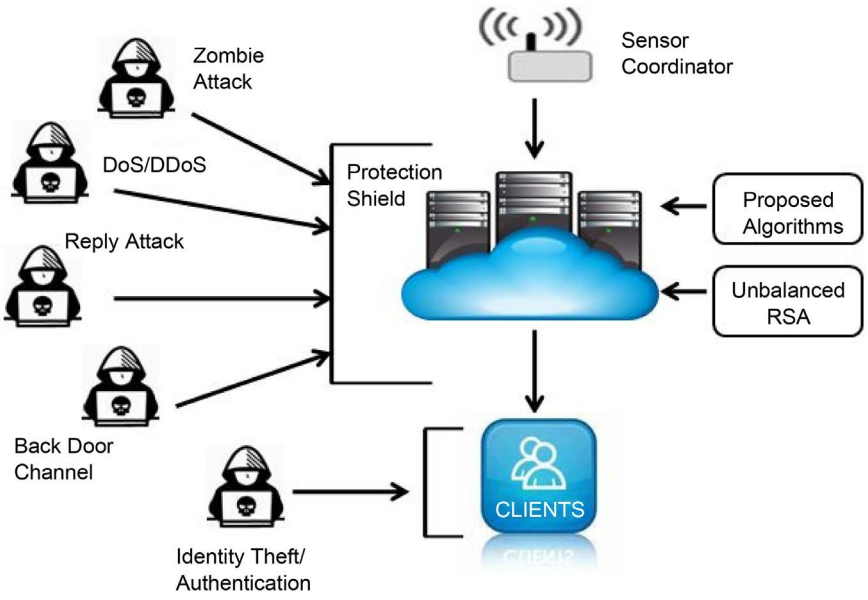

Figure 2. Proposed attack and mitigation method.

Table 3. Proposed mitigating algorithm for the multilayer framework.

Attacks/Threat Name	Mitigating Algorithm
Zombie Attack	
DoS/DDoS	Algorithm 1
Back door Attack	
Reply Attack	Algorithm 2
Authentication	Unbalanced RSA

Algorithm 1. Replay attack protection algorithm.

Algorithm: Replay_Attack_Protect (T_data, R_data, H, L)

Data: Transmitting data=T_data, Receiving data=R_data, Authorize bit=H, Unauthorized bit=L.
Result: Replay_attack=R_attack

(1) Start

(2) Connection==Serial Communication(); /*Check serial communication between router and coordinator*/

(3) If connection==Fail

(4) Return Start; /*Step 1*/

(5) End

(6) If connection==True then

(7) T_data==Encrypt(data); /*AES 128 bit encryption*/

(8) If R_data=='H' OR 'L' then /*128 bit decryption*/

(9) If R_data=='H' OR 'L'

(10) Initialization i, data;

(11) Fori=1 to 10 do

(12) Data=data+1;

(13) Delay==200 ms;

(14) If Data>7

(15) R_Attack==Yes;

(16) Update Web(R_attack); /*Update web page with Replay_attack data*/

(17) Send Email(Admin); /*Send email to Admin notifying Replay_attack*/

(18) Return Start; /*Step 1*/

(19) End

(20) End

(21) End

learning algorithms or signal processing techniques can be implemented using the vast variety of Python libraries built for those purposes. We have developed two algorithms which have been deployed in the own-cloud for mitigating the

Algorithm 2. Flooding attack protection algorithm.

```
Algorithm: Flooding_attack_protect (T_data, R_data, P, H, L)
Data: Transmitting data=T_data, Receiving data=R_data, Authorize bit=H, Unauthorized bit=L.
Result: Flooding_attack=F_attack.
(1) Start
(2) Connection==Serial Communication(); /*Check serial communication between router and coordinator*/
(3) If connection==Fail
(4) Return Start; /*Step 1*/
(5) End
(6) If connection==True then
(7) T_data==Encrypt(data); /*AES 128 bit encryption*/
(8) If R_data=='H' OR 'L' then /*128 bit decryption*/
(9) Initialization I, data;
(10) Fori=1 to 20 do
(11) Data=data+1;
(12) Delay==200 ms;
(13) If Data>7
(14) F_Attack==Yes;
(15) Update Web(F_attack); /*Update web page with Flooding attack data*/
(16) Send Email(Admin); /*Send email to Admin notifying Flooding attack*/
(17) Return Start; /*Step 1*/
(18) End
(19) End
(20) End
(21) End
```

attacks and threats to cloud-like reply attack, DoS/DDoS, back door attack, Zombie, etc. as mentioned in Algorithm 1 and Algorithm 2. We have used the unbalanced RSA algorithm to reduce the risk of authentication and authorization. All the proposed mitigation methods are tabulated in Table 3. Figure 2 represents the secured cloud system architecture after deploying the algorithms we have developed. The system was tested to evaluate the performance of mitigating the threats in a sensor network. The result shows that the framework can mitigate the threats properly.

6. Conclusion and Future Work

Security is one of the buzz word and major concerns in the information system especially in Cloud computing where sensitive applications and data are moved

into the cloud data centers. Cloud computing has several vulnerabilities like virtualization vulnerabilities, data vulnerabilities, and software vulnerabilities. With the improvement of Cloud computing technologies and the increasing number of cloud users, security dimensions are increasing continuously. Our main goal of the study is to provide protection for the user's valuable data, stored in the cloud from attackers or third-party authenticators. There are different types of security threats in cloud based services. It's complicated work to make a convergence platform to face security challenges. In this paper, we reviewed the literature for security challenges in Cloud computing and proposed a security model and a multilayer framework for secure Cloud computing environment that identifies security requirements, attacks, threats, concerns associated to the deployment of the clouds. Our proposed framework is modular in nature, means we consider the threats individually and seek solution for each of them. This helps to manage the cloud system more effectively and provides the administrator include the specific solution to counter the threat.

Acknowledgements

This work has been supported by Ministry of Science and Technology, Bangladesh, Financial Year 2020-2021, Special Grants from Science and Technology Program, GO No. 39.00.0000.009.06.009.20-1331/EAS-414, dated 8 Dec 2020.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Dikaiakos, M.D., Katsaros, D., Mehra, P., *et al.* (2009) Cloud Computing: Distributed Internet Computing for IT and Scientific Research. *IEEE Internet Computing*, **13**, 10-13. https://doi.org/10.1109/MIC.2009.103

[2] Băsescu, C., Carpen-Amarie, A., Leordeanu, C., Costan, A. and Antoniu, G. (2011) Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies. *Proceeding of IEEE International Conference on Advanced Information Networking and Applications* (*AINA*), Biopolis, Singapore, 22-25 March 2011, 459-466. https://doi.org/10.1109/AINA.2011.61

[3] Kumar, R.S. and Saxena, A. (2011) Data Integrity Proofs in Cloud Storage. 2011 *Third International Conference on Communication Systems and Networks* (*COMSNETS*), Bangalore, India, 4-8 January 2011, 1-4. https://doi.org/10.1109/COMSNETS.2011.5716422

[4] Wang, Z. (2011) Security and Privacy Issues within Cloud Computing. *International Conference on Computational and Information Sciences*, Chengdu, China, 21-23 Octorber 2011, 175-178. https://doi.org/10.1109/ICCIS.2011.247

[5] James, B.D., Elisa Bertino, J., Latif, U. and Ghafoor, A. (2005) A Generalized Temporal Role-Based Access Control Model. IEEE Computer Society, 2005

[6] Mukhin, V. and Volokyta, A. (2011) Security Risk Analysis for Cloud Computing Systems. *The 6th IEEE International Conference on Intelligent Data Acquisition*

and Advanced Computing Systems: *Technology and Applications*, Prague, Czech Republic, 15-17 September 2011.

[7] Mathisen (2011) Security Challenges and Solutions in Cloud Computing. 5*th IEEE International Conference on Digital Ecosystems and Technologies* (*IEEE DEST* 2011), Daejeon, South Korea, 31 May-3 June 2011, 208-212. https://doi.org/10.1109/DEST.2011.5936627

[8] La'Quata, S. (2010) Cloud Computing: Security Risk. Association for Computing Machinery, New York, USA. https://doi.org/10.1145/1900008.1900152

[9] Jensen, M., Sehwenk, J., *et al.* (2009) On Technical Security, Issues in Cloud Computing. 2009 *IEEE International Conference on Cloud Computing*, Bangalore, India, 21-25 September 2009, 109-116. https://doi.org/10.1109/CLOUD.2009.60

[10] Tripathi, A. and Mishra, A. (2011) Cloud Computing Security Considerations. *IEEE International Conference on Signal Processing*, *Communication and Computing* (*ICSPCC*), Xi'an, China, 14-16 September 2011, 1-5. https://doi.org/10.1109/ICSPCC.2011.6061557

[11] Jensen, M., Gruschka, N., *et al.* (2008) The Impact of Flooding Attacks on Network Based Services. 2008 *Third International Conference on Availability, Reliability and Security* (*ARES*), Barcelona, Spain, 4-7 March 2008, 509-513. https://doi.org/10.1109/ARES.2008.16

[12] Armbrust, M., Fox, A., Griffth, R., *et al.* (2009) Above the Clouds: A Berkeley View of Cloud Computing. Technical Report No. UCB/EECS-2009-28, University of California Berkeley, Berkeley, USA. https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[13] Okuhara, M., *et al.* (2010) Security Architecture for Cloud Computing. *Fujitsu Scientific & Technical Journal*, **46**, 397-402. https://pdfs.semanticscholar.org/488c/73323e8fe2fbd17988ec67b8838bb5ddc3ae.pdf

[14] (2010) Cloud Computing and Security—A Natural Match. Trusted Computing Group (TCG). https://trustedcomputinggroup.org/wp-content/uploads/Cloud-Computing-and-Security-Whitepaper_July29.2010.pdf

[15] Chow, R., Golle, P., Jakobsson, M., *et al.* (2009) Data in the Cloud: Outsourcing Computation without outsourcing Control. Proceedings of the first ACM Cloud Computing Security Workshop, CCSW 2009, Chicago, IL, USA, 13 November 2009, 85-90. https://doi.org/10.1145/1655008.1655020 http://markus-jakobsson.com/papers/jakobsson-ccsw09.pdf