International Journal of Grid and Distributed Computing
Vol.7, No.2 (2014), pp.89-98
http://dx.doi.org/10.14257/ ijgdc.2014.7.2.09

Security and Privacy Issues in Cloud Computing Environment: A Survey Paper

Kaleem Ullah and M. N. A. Khan

Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST)
Islamabad, Pakistan
kkqaisrani@yahoo.com, mnak2010@gmail.com

Abstract

Cloud computing is emerging as a powerful architecture to perform large-scale and complex computing. It extends the information technology (IT) capability by providing on-demand access to computer resources for dedicated use. The information security and privacy are the major concerns over the cloud from user perspective. This paper surveys and evaluates the architecture, data security and privacy issues in cloud computing like data confidentiality, integrity, authentication, trust, service level agreements and regulatory issues. The objective of this paper is to review comprehensively the current challenges of data security and privacy being faced by cloud computing and critically analyze these issues.

Keywords: *Cloud Computing, Data Security, Data Privacy, Authentication, Trust*

1. Introduction

Cloud computing is the next generation paradigm in computation, which is continuously growing and emerging. Cloud computing is a new era of computing which refers to both the applications and resources delivered on demand over the Internet as services. The hardware and software resources in the data centers that provide diverse services over the network or the Internet to address the user requirements are called "cloud" [3]. According to National Institute of Standards and Technology (NIST), cloud computing provides *a convenient on demand network access to a shared pool of configurable computing resources* [2]. Here, resources refer to computing applications, network resources, platforms, software services, virtual servers and computing infrastructure. The cloud computing can be conceived as a new computing archetype with an implication for greater elasticity and availability at a minimal cost. The three well-known and commonly used service models in the cloud paradigm are IaaS, PaaS and SaaS.

- **Infrastructure as a Service (IaaS):** The IaaS model provides the basic computing infrastructure of processing, storage and network resources where users can deploy and run arbitrary software. Its main purpose is to minimize the purchasing and managing cost of fundamental hardware infrastructure. The cloud subscriber is mainly responsible for the security of data except the underlying hardware infrastructure. The Amazon Elastic Compute Cloud (EC2) is an example of IaaS [11].

- **Platform as a Service (PaaS):** PaaS is a software deployment model where applications are developed and deployed on demand. It reduces the cost of software purchasing, housing and deployment. The security in this model is a shared

ISSN: 2005-4262 IJGDC

responsibility of cloud provider and the subscriber. The Amazon Simple Storage Service is an example of PaaS [10].

- **Software as a Service (SaaS):** The SaaS model provides software/application for use on demand. It reduces the cost of software, maintenance and operations. The security is the responsibility of the cloud provider in this model. The Google applications and salesforce.com are examples of SaaS [8, 9].

In other words, the cloud computing is an assortment of PaaS, SaaS and IaaS. The employees working for an organization can be users or providers of cloud computing services in accordance with the organizational scope and the control over the IT environment [1]. When a cloud is made available to the general public in a *pay-as-you-go* manner, it is called public cloud. Similarly, the term private cloud is used to refer to an internal data center of an organization or a corporate, which is not accessible to the general public. Similarly, the term hybrid cloud refers to a scenario where a private cloud and a public cloud are involved. The four well-known and commonly used cloud deployment models include [6, 7]:

- ***Public Cloud*** is a general purpose publicly available cloud model owned, operated and managed by the government organizations, academia, corporate and business enterprises or even a mix of them.

- ***Private Cloud*** is a model owned, operated and managed by a single organization or an enterprise for its employees or users.

- ***Hybrid Cloud*** is a combination of two or more distinct cloud infrastructure (*i.e.*, public, community or private) to share the cloud resources but maintains its unique entity.

- ***Community Cloud*** is a cloud infrastructure exclusively used by specific community users within an organization for a shared cause. It may be owned, operated and managed by themselves or a third party.

The cloud computing is an emerging era of computing which is facing many challenges of data protection and safety. Generally, the security is a joint responsibility of the cloud client and provider. However, the organization itself is accountable for its all resources over the cloud. Although the cloud computing offers many benefits, for instance, low cost, but the data security and privacy issues pose serious concerns. To identify these issues, this paper presents a survey on the current security and privacy issues in the cloud computing.

The rest of this paper is structured as follows: Section II provides literature review. The critical evolution is covered in section III. The gap analysis on the issues that still remain unanswered is given in section IV and finally, conclusion and future work are described in the last section.

2. Literature Review

The primary motivation for adopting cloud is its low cost; however, on the other side, enterprise becomes responsible and accountable for overall security of the outsourced services [12]. The key security issues pertinent to cloud computing are organized into several categories such as data protection, trust, identity management, architecture, software isolation and availability. The organization must consider the potential security threats before adopting the cloud. The security of cloud infrastructure

mostly depends on trusted computing and cryptography. The business or enterprise data must be protected with appropriate and reliable policies or procedures, whether in the enterprise's own data center or in the cloud environment. Such an approach acts as a starting point with a list of common outsourcing requirements like Security and Privacy Standards, Compliance and Regulatory Issues, Service Level Agreements (SLAs), Certificates, etc. Moreover, the risk management is also necessary for the business enterprises before migration to cloud. The risk must be carefully mitigated because the organization is accountable for its resource security.

The audit, SLAs, certifications and risk treatment methods being an important structural chunk of cloud security and controls are defined into a single framework in [13]. An Information Security Management System (ISMS) consists of policies, processes and mechanisms that an enterprise utilizes to establish, implement, operate, monitor and improve the information security. The framework referred to virtual ISMS is compared with the conventional ISMS for those organizations where IT services are somewhat outsourced. The virtual ISMS is, in fact, a structured way to manage risk and organizational assets over the cloud. Moreover, as cloud client and provider are jointly responsible for data security and control in the cloud, so they can adopt virtual ISMS as a standard complaint management process for the protection of shared assets. Thus, it is more important from the client's perspective that they should be cognizant of what they are purchasing with cloud.

Mohammad [14] highlighted the significant key drivers and constraints for secure cloud computing from a societal and technical perspective. The trust, privacy and user approach towards cloud computing are the social issues while on the other side encryption, scalability, reliability, data rights and transparency are the stern technological issues in cloud computing. Most of the cloud users are unaware of the risk of storing and transmitting private information in a shared environment. Therefore, key technological constraints like compliance, transparency, encryption, integrity and multi-tenancy should be addressed carefully. The transparency is the biggest challenge for the enterprises at present, and due to this, they are reluctant to switch to cloud computing environment. Once the cloud becomes transparent and the users have full control to access, manage and report pertaining to the state of data and services, only then it will help increase the trust and minimize the social and technological constraints.

The inherent issues of data security, governance and management with respect to control in the cloud computing are discussed in [15]. The major issues in cloud data security are: data privacy, data protection, data availability, data location and secure transmission. The issue of storing data over the trans-boarder servers is a serious concern of clients as cloud venders are governed by the local laws and, therefore, the cloud clients should be cognizant of those laws. The data availability is also an important concern and service downtime must be according to the predefined SLAs. Moreover, the cloud provider should ensure the data security, particularly data confidentiality and integrity. The cloud provider should share all such concerns with the client and a build trust relationship in this connection. The cloud vender should provide guarantees of data safety and explain jurisdiction of local laws to the clients. The main focus in the paper is on those data issues and challenges which are associated with data storage location and its relocation, cost, availability and security.

The privacy risk associated with cloud computing has raised serious questions [16]. Therefore, the cloud providers should put in place clear and transparent procedures and policies with respect to the legal framework in order to win the trust of the customers.

And due to the same reasons, the users should evaluate carefully the data security and privacy issues before stepping into the arena of cloud computing. Furthermore, the legal jurisdiction issues related to data in domestic and trans-border clouds should also be considered. These issues must be addressed and negotiated with mutual understanding in the befitting manners. When multiple users use the cloud over the trans-border then it increases the legal jurisdiction burden and the responsibility of cloud provider. In this context, the consumer's risk and rights need to be addressed and understood appropriately. Moreover, it is necessary for consumers to know the cloud provider's local laws related to data privacy and protection. The cloud provider has to develop and make data protection procedures, policies and laws and then create awareness about such laws among the users.

The cost effectiveness is one of the major motivations for the organizations willing to switch to the cloud computing irrespective of across-the-board security analysis of the cloud provider. The Identity and Access Management (IAM) protocols and standards are the important data security aspects discussed in [17]. The IAM is an adequate level of protection for organizational assets through implementing appropriate policies. The emerging IAM challenges can be minimized through discussing authentication, authorization and auditing issues. The IAM life cycle consist on five stages: *Provisioning and Deprovisioning, Authentication and Authorization, Self-Service, Password Management, and Compliance and Audit.* Furthermore, different standards and protocols like Security Assertion Markup Language (SAML) and Open Authentication (OAuth) protocol are used to mange identities in the cloud. To this end, the organizations must prepare IAM strategy, structure and understand the IAM life cycle before migrating to cloud. The IAM should also be properly implemented to ensure the mutual authentication, auditing and authorization for cloud computing management.

The cloud computing is becoming a popular and attractive paradigm with lots of benefits; however, there are some specific questions relating to its ability to support forensic investigation [18]. The author mainly discussed the cloud characteristics, models, and architecture. The forensic investigation has its roots for data recovery to finding digital evidence from law enforcement perspective. In cloud computing, the forensic readiness is not thoroughly considered by most of the organizations, so there is a need to revisit or develop new procedures to meet the current cloud requirements. Moreover, the forensic investigation has pros and cons, which need to be understood during forensic readiness. Similarly, the forensic investigation finding in virtual machines (VMs) has mixed approach of advantages and disadvantages. Therefore, the forensic investigator community is required to develop new procedures and techniques to overcome the cloud computing forensic analysis challenges.

The data confidentiality, authentication and access control issues in cloud computing have been addressed by proposing a framework to increase the cloud reliability and trustworthiness in [19]. A cryptographic algorithm Diffie-Hellman for secure communication, in contrast to key distribution management, is proposed in [24]. Such a system normally consists of three modules: administration, authentication and encryption modules. Each module has different, but interconnected, functions. The administration module is used by the cloud provider for user registration and administration. While the authentication module is used for authentication of users, and encryption module is used for data encryption. The authentication realization is a two-way process. Firstly, the system requires the user to enter normal login and password, and then it generates one-time password and sends it on the user mobile for

authentication. Once the one-time password is supplied, the system authenticates the user and grants access to the system.

The proposed system was tested on Java Remote Method Invocation (RMI) in cloud environment [42]. The system eliminates the cloud overload and prevents it from man in the middle attack.

Mirashe *et al.* [20] discuss the cloud computing service and deployment models and highlight their advantages. The authors further define the classes of cloud users, e.g., families, community and corporations. According to the authors, data protection is the major issue in cloud computing. The customer's data could be prone to serious threats if it is kept unencrypted on disk or memory or over the network in the cloud. The second major concern is related to the auditing of public cloud. The cloud providers are usually reluctant to undergo auditing for their resources and infrastructure. The last but not least issue is legal jurisdiction over the cloud. It is recommended that the enterprises should consider these issues before adopting cloud computing environment.

Sun *et al.* [21] highlight the key security, privacy and trust issues in existing environment of cloud computing and help users to recognize the tangible and intangible threats associated with its use. According to the authors, there are three major potential threats in cloud computing, namely the security, privacy and trust. Security plays a vital role in current era of long dreamed vision of computing as utility. It can be divided into four sub-categories: safety mechanisms, cloud server monitoring or tracing, data confidentiality and avoiding malicious insiders' illegal operations and service hijacking. Furthermore, the authors highlight the importance of data privacy in cloud computing. It is a key point from user perspective; therefore, it is vital to understand its allied issues like user control over the data and legal jurisdiction requirements. Moreover, the trust is a complex relationship between cloud client and provider, and it should be planned prior to adopting the cloud milieu. The trust between cloud provider and client should be reliable and measurable to make the trustworthy decisions. The trust can be divided into four sub-categories: trust evaluation, trust relationship, trust degree and trust monitoring.

The security control measurements in cloud computing are equivalent to the ones in the conventional IT set up [22]. The client should know answers to the seven safety questions prior to making the selection of cloud providers. These questions pertain to data location, data segregation, recovery, privileged user access, regularity compliance, forensic support and viability on a long-term basis. Moreover, the client has to exclusively analyze the data privacy, protection and security problems throughout the data life cycle over the cloud. The data life cycle passes through seven phases: data generation, transfer, use, share, storage, archival and destruction. The data identification, data isolation and privacy protection are the primary concerns and must be kept into consideration during the design and development of cloud-based applications. The integrated and complete security solutions are expected to meet the data security and protection objective in depth.

Kandukuri *et al.* [23] discussed importance of the legal agreements between the service provider and client. The cloud service provider can secure trust of a client through SLAs and service quality. A typical SLA normally consists of eight main contents, including Definition of Service, Performance Management, Problem Management, Customer Duties and Responsibilities, Security, Disaster Recovery and Business Continuity and Termination. Furthermore, the SLA should also describe how the security in the cloud is maintained and what are the methods and procedures used in maintaining security to make it client compliant. The basic security concerns that SLA

should contend with include: privileged user access, regulatory compliance, forensic analysis support, data location/relocation and data segregation, data recovery and viability. The present-day SLAs encompass only the subject of services provided, and waivers are offered in case the desired services do not meet the agreement. However, these waivers do not really help the customer's losses. Moreover, the SLA should also discuss other problems like data security policies, methods, procedures and their successful execution.

Khan *et al.*, [25, 26] proposed a machine learning approaches for post-event timeline reconstruction. The proposed techniques however are based on static analysis of the data enclosures. Iqbal *et al.*, [27, 28] proposed performance metrics for software design and software project management. Process improvement methodologies are elaborated in [29, 30] and Khan *et al.*, [31] carried out quality assurance assessment. Amir *et al.*, [32] discussed agile software development processes. Khan *et al.*, [33] analyzed issues pertaining to requirement engineering processes. Umar and Khan [34, 35] analyzed non-functional requirements for software maintainability. Khan [36] suggests that Bayesian techniques are more promising than other conventional machine learning techniques for timeline reconstruction. Rafique and Khan [37] explored various methods, practices and tools being used for static and live digital forensics. In [38], Bashir and Khan discuss triaging methodologies being used for live digital forensic analysis. Shahzad *et al.*, [39] proposed a novel technique to protect systems form malware attacks. Zia *et al.*, [40, 41] proposed a technique to reduce response time in cloud environment.

3. Critical Evaluation

The data security and privacy are the prime concerns in cloud computing. The security issues differ from each other due to the nature of threat, requirements and applicability. A comparative evaluation based on the above security and privacy aspects is presented in Table-1. We have critically reviewed the literature based on the following areas of security and privacy in the cloud paradigm:

- Trust and Compliance.
- Confidentiality, Integrity, Authentication and Availability.
- Procedure, Policy, SLAs and Virtual ISMS.
- Data Protection/Recovery and Auditing.
- Risk Analysis.

The trust and compliance are the complex relationship between the cloud client and provider. The cloud provider can gain trust with the client by offering open SLAs, legal jurisdiction and data recovery/auditing facilities. The proper SLAs with detailed procedures can also be used to address the security concerns of the cloud clients. These SLAs must be predefined and thoroughly negotiated by both the parties [12].

Similarly, the proper cryptographic algorithms, hash function and IAM techniques can provide data confidentiality, integrity and authentication during data transmission. The guarantee of data protection during all modes of transaction is very important from client's point of view. Thus, the cloud provider has to ensure the safety, auditing and privacy of data [17].

Moreover, the risk management is vital and enterprises must perform periodic risk analysis. However, the virtual ISMS becomes crucial in the absence of conventional ISMS.

The virtual ISMS is important because it regulates the procedures, policies, controls and SLAs, etc., which are useful for both the cloud client and provider [13, 14].

The trust, data architecture, identity management, data protection, software isolation, and availability are the key area of interest discussed in [15]. A system for data encryption, authentication and data integrity is proposed in [19]. Svantesson and Clarke [16] discussed simple cloud security problems. The core issues of trust, compliance, risk management, virtual ISMS, data privacy, confidentiality, integrity and availability are discussed in [18, 22].

Table-I. Critical Evaluation of Security and Privacy Issues in Cloud Computing

Ref	Research Theme	Issues Discussed	Proposed Solution	Strength/Benefits	Scope
Jansen [12]	Security and Privacy issues in Cloud Computing	Trusted and reliable computing	Service Level Agreements, Policies and Procedures, Risk Management.	Data Security and Privacy will be ensured	Limited to addressing technical issues
Julisch [13]	Security and Control in Cloud Computing	Security and controls concerns	Service Level Agreements, Virtual Information, Security Management System (ISMS).	Standard compliant management process and assets protection will be ensured	Limited to addressing the management and controls issues
Mohammed [14]	Secure Cloud Computing	Social and Technological Constraints	Proposed a solution to address Compliance, Transparency, Encryption and Multi-tenancy.	Data privacy will be ensured	Limited to addressing social and technical issues
Mehmood [15]	Security and Data Storage Location in Cloud Computing	Data issues of storage location, cost, availability and security	Appropriate use of cloud technologies.	Data storage location and availability will be ensured	Limited to addressing data storage location issues
Svantesson [16]	Risk in Cloud Computing	Legal Regulatory Aspects and Consumer Rights	Improvement in consumer rights and privacy laws.	Consumer rights protection will be ensured	-
Almulla [17]	Security Management in Cloud Computing	Data Security and Identity and Access Management (IAM)	A solution to address Identity Management-as-a-Service (IDaaS).	Authentication, Authorization and auditing will be ensured	Limited to discussing the identity and access management
Relly [18]	Forensic Investigation for Cloud Computing	Computer Forensic from Law Enforcement prospective Pros and Cons of Forensic	-	Law Enforcement	Scope to improve and develop forensic procedures and tools
Patil [19]	Data Security in Cloud Computing	Data Access Control	A solution to address authentication mechanism.	Security, privacy and compliance will be ensured	Limited to addressing access control issues
Chen [22]	Security Controls in Cloud Computing	Life Cycle Data on Cloud	Data Security and Privacy.	Data Identification, Isolation and Privacy protection will be ensured	-
Kandukuri [23]	Service Level Agreements for Secure Cloud	Client Compliance and Trust	Compliance, Trust, Data Segregation and Recovery.	Data security policies and procedures will be ensured	Scope to design standard SLAs

4. Gap Analysis

The gap analysis is a tool that helps identify and compare the gap between present status and the potential status in certain fields of study. The purpose of gap analysis into the area of information technology, especially in cloud computing, is to look at the probable issues of data security and privacy. During the phase of literature review in this study, we have found the following gaps in the area of cloud computing with respect to security and privacy issues.

a. Absence of appropriate business support standards which include:
   - Standards for cloud SLAs and quality of services.
   - Standards for cloud service resources.
   - Standards for service consumptions and usage.

b. Lack of standard for security and privacy that include:
   - Identity management across multiple networks and administration domains.
   - For secure and efficient replication of identity and access policy information across systems.
   - For single sign-on interface that supports strong authentication.
   - Policies, processes, procedures and technical controls in supporting the security auditing, regulation and law compliance needs.

6. Conclusion

The cloud technology is advancing rapidly and enterprises are speedily adopting it. The cloud cost and performance are the major benefits; however, some basic security problems have ebbed into the background. The cloud computing is associated with some serious risk to privacy and consumer rights. Consequently, the organizations dealing with cloud computing must address the key security issues like trust, confidentiality, integrity, authentication, control and audit, risk analysis, SLAs, procedure and policies, ISMS and laws to enhance the efficiency of the cloud. The Chief Information Officers (CIOs) and Chief Security Officers (CSOs) of the cloud user and provider sides need to comprehend and address the risk and security issues in detail before actually benefiting its high-end computing power.

References

[1] Y. Chen, V. Paxson and R. H. Katz, "What's New about Cloud Computing Security?", Technical Report No. UCB/EECS-2010-5, Electrical Engineering and Computer Sciences University of California at Berkeley, **(2010)** January 20.
[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", version 15, National Institute of Standards and Technology (NIST), Information Technology Laboratory, www.csrc.nist.gov, **(2009)** October 7.
[3] N. Leavitt, "Is Cloud Computing Really Ready for PrimeTime?", IEEE Computer, **(2009)** January.
[4] L. M. Vaquero1, L. Rodero-Merinol, J. Caceres and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition", Computer Communication Review, January 2009, http://ccr.sigcomm.org/online/files/p50-v39n1l-vaqueroA.pdf.
[5] L. Youseff, M. Butrico and D. D. Silva, "Toward a Unified Ontology of Cloud Computing", Grid Computing Environments Workshop, held with SC08, **(2008)** November,http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf.
[6] D. Linthicum, "Cloud Computing? Thank SOA", [Online] Available at: http://www.thecloudtutorial.com/cloud-computingsoa.html.

[7] J. M. Willis, "Cloud Computing and the Enterprise", IT Management and Cloud, [Online] Available at: www.johnmwillis.com/ibm/cloud-computing-and-the-enterprise/, **(2008)** February 13.
[8] Google Apps, "Get online email, calendar documents and more working for your organization", http://www.google.com/apps/index1.html.
[9] Salesforce, "Software as a service – SaaS", http://www.salesforce.com/saas/.
[10] Amazon, "Amazon Simple Storage Service (Amazon S3)", http://aws.amazon.com/s3/.
[11] Amazon, "Amazon Elastic Compute Cloud (Amazon EC2)", http://aws.amazon.com/ec2/.
[12] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44th Hawaii International Conference on System Sciences - 2011, IEEE.
[13] K. Julisch and M. Hall, "Security and Control in the Cloud", Information Security Journal: A Global Perspective, vol. 19, **(2010)**, pp. 2099-309.
[14] D. Mohammed, "Security and Cloud Computing: An Analysis of Key Drivers and constraints", Informatio Security Journal: A Global Perspective, vol. 20, **(2011)**, pp. 123-127.
[15] Z. Mehmood, "Data Location and Security Issues in Cloud Computing", International Conference on Emerging Intelligent Data and Web technologies, IEEE, **(2011)**.
[16] D. Svantesson and R. Clarke, "Privacy and Consumer Risks in Cloud Computing", Computer Law and Security Review, vol. 26, **(2010)**, pp. 391-397
[17] S. A. Almulla and C. Y. Yeun, "Cloud Computing Security Management".
[18] D. Relly, C. Wren and T. Berry, "Cloud Computing: Pros and Cons for Computer Forensic Investigations", International Journal Multimedia and image Processing (IJMIP), vol. 1, issue 1, **(2011)** March, pp. 26-34.
[19] D. H. Patil, R. R. Bhavsar and A. S. Thorve, "Data Security over Cloud", International Journal of Computer Applications® (IJCA), **(2012)**.
[20] S. P. Mirashe and Dr. N. V. Kalyankr, "Cloud Computing", Journal of Computing, vol. 2, issue 3, **(2010)** March.
[21] D. Sun, G. Chang, L. Sun and X. Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environment", Procedia Engineering, vol. 15, **(2011)**, pp. 2852-2856.
[22] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", 2012 International Conference on Computer Science and Electronics Engineering, IEEE.
[23] B. R. Kandukuri, R. Paturi V and Dr. A. Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing, IEEE.
[24] RSA Laboratories, "The Diffie-Hellman key agreement protocol", http://www.rsa.com/rsalabs/node.asp?id=2248.
[25] M. N. A. Khan, C. R. Chatwin and R .C. Young, "A framework for post-event timeline reconstruction using neural networks. digital investigation, vol. 4, no. 3, **(2007)**, pp. 146-157.
[26] M. N. A. Khan, C. R. Chatwin and R .C. Young, "Extracting Evidence from Filesystem Activity using Bayesian Networks", International journal of Forensic computer science, vol. 1, **(2007)**, pp. 50-63.
[27] S. Iqbal, M. Khalid and M. N. A. Khan, "A Distinctive Suite of Performance Metrics for Software Design", International Journal of Software Engineering & Its Applications, vol. 7, no. 5, **(2013)**.
[28] S. Iqbal and M. N. A. Khan, "Yet another Set of Requirement Metrics for Software Projects", International Journal of Software Engineering & Its Applications, vol. 6, no. 1, **(2012)**.
[29] M. Faizan, S. Ulhaq and M. N. A. Khan, "Defect Prevention and Process Improvement Methodology for Outsourced Software Projects", Middle-East Journal of Scientific Research, vol. 19, no. 5, **(2014)**, pp. 674-682.
[30] M. Faizan, M. N. Ahmed and S. Ulhaq, "Contemporary Trends in Defect Prevention: A Survey Report", International Journal of Modern Education & Computer Science, vol. 4, no. 3, **(2012)**.
[31] K. Khan, A. Khan, M. Aamir and M. N. A. Khan, "Quality Assurance Assessment in Global Software Development", World Applied Sciences Journal, vol. 24, no. 11, **(2013)**.
[32] M. Amir, K. Khan, A. Khan and M. N. A. Khan, "An Appraisal of Agile Software Development Process", International Journal of Advanced Science & Technology, vol. 58, **(2013)**.
[33] A. Khan, M. Naeem, M. Khalid and S. ul Haq, "Review of Requirements Management Issues in Software Development", International Journal of Modern Education & Computer Science, vol. 5, no. 1, **(2013)**.
[34] M. Umar and M. N. A. Khan, "A Framework to Separate Non-Functional Requirements for System Maintainability", Kuwait Journal Of Science & Engineering, vol. 39, no. 1 B, **(2012)**, pp. 211-231.
[35] M. Umar and M. N. A. Khan, "Analyzing Non-Functional Requirements (NFRs) for software development", In Software Engineering and Service Science (ICSESS), 2011 IEEE 2nd International Conference, IEEE, **(2011)** July, pp. 675-678.
[36] M. N. A. Khan, "Performance analysis of Bayesian networks and neural networks in classification of file system activities", Computers & Security, vol. 31, no. 4, pp. 391-401.
[37] M. Rafique and M. N. A. Khan, "Exploring Static and Live Digital Forensics: Methods, Practices and Tools".

[38] M. S. Bashir and M. N. A. Khan, "Triage in Live Digital Forensic Analysis", International journal of Forensic Computer Science, vol. 1, **(2013)**, pp. 35-44.
[39] A. Shahzad, M. Hussain and M. N. A. Khan, "Protecting from Zero-Day Malware Attacks", Middle-East Journal of Scientific Research, vol. 17, no. 4, **(2013)**, pp. 455-464.
[40] A. Zia, A. Khan and M. Naeem, "Identifying Key Challenges in Performance Issues in Cloud Computing", International Journal of Modern Education & Computer Science, vol. 4, no. 10, **(2012)**.
[41] A. Zia and M. N. A. Khan, "A Scheme to Reduce Response Time in Cloud Computing Environment", International Journal of Modern Education & Computer Science, vol. 5, no. 6, **(2013)**.
[42] Oracle Technology Network, "Java Remote Method Invocation (RMI)", http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136424.html.

Authors

Kaleem Ullah is pursuing for MS in Information Security Management at Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad, Pakistan. He obtained his Master's Degree in Information Technology from Gomal University, D.I. Khan, Pakistan in 2004. He has 6+ years of extensive work experience in the field of Information Technology. His research interests include Information Security, Cyber Threats and Cloud Computing.

M. N. A. Khan obtained D.Phil. degree in Computer System Engineering from the University of Sussex, Brighton, England. His research interests are in the fields of software engineering, cloud computing, cyber administration, digital forensic analysis and machine learning techniques.

