International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.155-166
http://dx.doi.org/10.14257/ijsia.2015.9.11.16

Ensuring Data Confidentiality and Authentication through Encryption at Application Layer

Kaleem Ullah, 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 has emerged as a powerful and viable architecture to meet large-scale and complex computational needs of the organizations. It extends the IT capability by providing on-demand access to computer resources for dedicated use. Data security and privacy are the major concerns over the cloud from user perspective. Consequently, the organizations which deal with cloud computing should amicably address the key data security risks. In this paper, a generic scheme of user authentication and data confidentiality has been introduced. We introduce a tool that encrypts/decrypts the user data at application layer using public key infrastructure. The information security experts of both the sides i.e. cloud users and service providers must comprehend and address the risk and security issues in detail before actually benefiting high-end computing power offered by the cloud computing paradigm.

***Keywords**: Cloud Computing, Data Security, Confidentiality, Authentication, Public Key Infrastructure, Encryption*

1. Introduction

Cloud computing is an emerging computing arena which refers to on demand delivery of both the applications and resources in the form of services over the Internet. The hardware and software resources in a data center that provide diverse services over the Internet are called "cloud" [1]. According to NIST, cloud computing provides *a convenient on demand network access to a shared pool of configurable computing resources* [2]. Here, the term "resources" refer to computing applications, network resources, platforms, software services, virtual servers and computing infrastructure.

Generally, the data security is a joint responsibility of the client and cloud vendor. Nevertheless, the client itself is solely accountable for security of all its resources over the cloud. Although cloud computing offers several benefits, especially the low cost computing, but the data security and privacy issues are of serious concerns in this paradigm. There are several conventional methods to secure data as described below.

1.1 Cryptography

Cryptography is an effective way to protect information. It is a method of transmitting and storing data in such a way that only the authorized user can access and process it. The commonly used generic terms in cryptography are plaintext (readable data), cyphertext (unreadable data), encryption (conversion process), decryption (reverse conversion process) and algorithm (set of rules used for data encryption and decryption). Figure 1 illustrates the conventional encryption and decryption procedure.

ISSN: 1738-9976 IJSIA

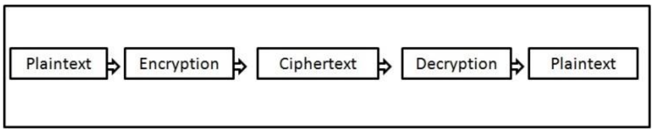

Figure 1. Generic Encryption/Decryption Procedure.

The implementation of pure cryptographic process in the form of hardware or software is termed as cryptosystem. The following six security services are offered by a cryptosystem [3]:

- ***Confidentiality*** is used to ensure that information is meaningless for unauthorized users.
- ***Integrity*** is used to ensure that information is complete and tamper proof.
- ***Authentication*** is used to ensure the entity claim of both the ends is correct and true.
- ***Digital Signature*** is used to ensure identity of the sender.
- ***Non-repudiation*** is the ability for a system to ensure that no user can deny from his/her actions.
- **Availability** pertains to the accessibility of transmission media (network, hardware/software).

Two kinds of encryptions, *symmetric key encryption* (shared secret) and *asymmetric key encryption* (public key), are widely used in cryptography [6].

- *Symmetric Key Encryption*: Symmetric encryption algorithm makes use of single key for data encryption and decryption much alike Advanced Encryption Standard (AES). The AES is a symmetric/single key algorithm, meaning the similar key is applied for data encryption and decryption. The AES algorithm contains 128 bits fixed block size with a key size of 128, 192, and 256 bits.
- *Asymmetric Key Encryption*: Asymmetric encryption employs pair of two different interconnected keys (public and private). Data encrypted through one key is decrypted through its opposite corresponding key.

1.2 Public Key Infrastructure (PKI)

PKI consists of various procedures, communication protocols, policies and cryptographic algorithms to ensure secure communication among distinct entities in a comprehensive manner. In other words, PKI is a mechanism that provides security services or features including user authentication, data confidentiality, non-repudiation and digital signature. In a system employing PKI, each user possesses two types of keys. First is known as **public key** and the second is known as **private key**. In PKI, a user's digital identity authenticates over a public or private network. These two keys are generated using a cryptographic algorithm and shared through a certificate authority (CA) that mathematically links them to establish the user's unique identity. In PKI systems, private key is always kept secret by the end user and is never transmitted over the network, while its corresponding public key is distributed unrestrictedly over the network.

There are five main components of PKI [4]:

- End Entity (EE) is a general term used to represent end users, devices (servers, router) or any other entity which is legitimately utilized to support PKI related services.
- Certificate Authority (CA) is an entity which digitally signs and issues a certificate containing an identity and a key. A trusted third party such as VeriSign or one or more in house servers can provide CA functionality.

- Certificate Repository (CR) serves as a storage repository for certificates, and these certificates can be accessed on demand by the End Entities.
- Registration Authority (RA) is an elective module that performs multiple administrative tasks for CA. The RA is usually linked with end user certificate registration method.
- Certificate Revocation List (CRL) is also an elective component in which CA can delegate to publish CRLs.

As stated earlier, the six key traits of secure communication are: confidentiality, integrity, authentication, digital signature, non-repudiation and availability; and among them the most important is authentication [5]. Authentication is the procedure to verify the identity of a user and is based on three different factors. These factors are something that a user knows, something the user possesses and something the user itself is. Something a user knows means password that is a communal clandestine among issuing entity and the user. Something the user possesses could be a physical token or digital signature like private key. This form of authentication is generally called two-factor authentication. Something the user itself is could pertain to a fingerprint, DNA or retinal scan which is unique to every user.

1.3 OSI Model

The Open System Interconnection (OSI) model was designed in 1984 by the International Organization for Standardization. The OSI reference model is the networking framework which comprises on a set of seven layers to implement different protocols on diverse stages. It is a conceptual framework in which the data is passed through upper most application layer to bottom most physical layer one by one at sending end, and the reverse process takes place at the receiving end. The OSI model performs the task of internetworking and ensures that data must pass through from a single device to a different device over a network.

The model is divided into a vertical stack that contains the following seven layers:

- ***Application Layer*** describes, identified and establishes the intended communication partner by interacting with the OS. It also determines availability of the adequate resources for the intended communication.
- ***Presentation Layer****,* occasionally called syntax layer, implements coding and conversion functions such as compression/decompression or encryption/decryption to make a standard format for other layers.
- **Session Layer** sets up, maintains and terminates connections/sessions between presentation layer entities and provides dialogue control among nodes. This layer has three kinds of communication modes: simplex, half-duplex and full-duplex.
- ***Transport Layer*** preserves data flow control and performs error checking and recovery of data between two end points of the network connection. It supports both reliable and unreliable data transportation services. This layer has three *flow control* methods: buffering, windowing, and congestion prevention.
- ***Network Layer*** defines how data can be exchanged and delivered between any two nodes in a network. This layer describes the reasonable protocols, addressing and routing structure of the network.
- ***Data Layer*** defines the logical organization of data and maintains media access.
- ***Physical Layer*** is actual hardware that provides physical properties of the various communication media. It describes the physical characteristics of the network like connections, voltage levels and timing.

1.4 Cloud Computing

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. The four known cloud deployment models include public, private, hybrid and community cloud. Cloud computing is facing several challenges relating to data security protection and privacy issues. To overcome such issues, this paper presents a PKI and cryptography based framework.

Rest of the paper is organized as follows. Section II discusses related work. The problem statement and research motivation is covered in section III. The proposed security model is described in Section IV and the experiments conducted for this research are outlined in Section V. Finally the conclusion along with the probable future work is described in the last section.

2. Literature Review

The primary motivation for cloud adoption is its low cost. However, on the other side, enterprise becomes responsible and accountable for overall security of the outsourced services [7]. 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 security of cloud infrastructure mostly depends on trusted computing and cryptography. 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 [8]. 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. Thus, it is more important from the client’s perspective that they should be cognizant of what they are purchasing with cloud.

Mohammad [9] 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. 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 at length in [10]. The major issues in cloud data security are: data privacy, protection, availability, 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 privacy risk associated with cloud computing has raised serious questions [11]. Therefore, the cloud providers should put in place clear and transparent procedures and policies with respect to the legal framework in order to win trust of the customers. 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 Identity and Access Management (IAM) protocols and standards are the important data security aspects discussed in [12]. The emerging IAM challenges can be minimized through contemplating on authentication, authorization and auditing issues. The IAM life cycle consist on five stages: *Provisioning and De-provisioning, 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. The IAM should be properly implemented to ensure the mutual authentication, auditing and authorization for cloud computing management.

The new emerging type of computing called 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 [13]. 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. Therefore, the forensic investigating community is required to develop new procedures and techniques to overcome the cloud computing forensic analysis challenges.

Data confidentiality, authentication and access control issues in cloud computing are addressed in [14] by proposing a framework to increase the cloud reliability and trustworthiness. In contrast to key distribution management, a cryptographic algorithm Diffie-Hellman for secure communication is proposed in [19]. Such a system normally consists of three modules: administration, authentication and encryption modules. 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 code and sends it to the user mobile for authentication. Once the correct one-time code is supplied, the system authenticates the user and grants access to the system. A similar system was proposed in [16] and tested on Java Remote Method Invocation (RMI) in the cloud environment.

The customer’s data could be prone to serious threats if it is kept unencrypted on disk or over the network in the cloud. Mirashe *et al.* [15] discuss the cloud computing service and deployment models and highlight their advantages. Another major concern is related to the auditing of public cloud since the cloud providers are generally reluctant to undertake auditing for their resources and infrastructure.

Sun *et al.* [16] discuss the key issues of data security and its privacy in cloud computing and emphasize comprehension of the tangible and intangible intimidations linked with its utilization. There are three major potential threats in cloud computing: security, privacy and trust. The trust between cloud provider and client should be reliable and measurable to make the trustworthy decisions.

The security control measurements in cloud computing are equivalent to the ones in the conventional IT setup [17]. The data lifecycle on the cloud passes through seven phases: data generation, transfer, use, share, storage, archival and destruction. The data identification, data isolation and privacy protection are the primary key concerns and should be kept into consideration during the design and development of cloud-based applications.

Kandukuri *et al.* [18] discuss importance of the legal agreements between the service provider and the client. The cloud service provider can secure trust of a client through SLAs and service quality. The basic security concerns that SLA should be 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 compensate the customer’s losses. References [20-51] reviewed different techniques in different domains and reported their critical evaluations along with a workable framework where necessary.

3. Problem Statement and Research Motivation

The gap analysis help identify the shortfalls of security issues in cloud computing. The gap analysis helped us understanding the issues of data security and privacy, and based on the gap analysis, we decided to find answer to the following question: *How can data confidentiality and authentication over network using encryption tool be efficiently achieved?*

Finding answer of the above question serves as the primary motivation to conduct this research and for this purpose we have designed and proposed a cryptographic based tool using JavaScript and HTML5. A framework is designed to ensure data privacy and authentication. Our proposed security framework has been validated through experiment.

4. Proposed Model

In cloud computing, data security is the major concern from users' point of view and one way to obtained maximum security is to keep and transmit encrypted data over the network. Therefore, we proposed to achieve two security services *authentication* and *confidentiality* in order to make data more secure. The data security and privacy are the key issues now-a-days, but this is the matter of compromise vs completely lock down. The proposed framework is envisaged to permit various users to select their files from their own computers and encrypt those file with long passwords at client-end. In our framework, we use the HTML5 API (FileReader), and an encryption library called CryptoJS of JavaScript to make this workable. Our proposed application does not encrypt the actual file, but our application creates a copy of it. In this way, we do not lose the actual file. For this purpose firstly we develop an encryption/decryption tool and then build a web server. We have proposed the following model to achieve data security though own developed tool.

The proposed model is designed to get the answer of the earlier stated research question by describing the following details:

- User authentication/authorization through web server
- Data confidentiality through software based encryption/ decryption tool which works at application layer.

The model consists on the following four major components:

4.1 Authentication/Authorization

For user authentication, we use network and build a local domain and web server. The user is created on the domain and added into web server. Whenever, a user has required to accessing the SSP to fetch or store data; he/she always has to present his certificate to the SSP. Then user's identity will be confirmed through his certificate with ACM (Access Certificate Matrix). If the user is authenticated, access to SSP will be granted after confirming the validation of the user and his/her certificate. After that, a user can download or upload his encrypted data over the cloud. The client should know answers to the seven safety questions prior to making the selection of cloud providers. 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.

4.2 Storage Server

The organization can maintain the storage services for storing its encrypted data in local ISP. The local ISP provides storage space to its clients. The SSP has to maintain client provided user Access Certificate Matrix (ACM) for user authentication. This ACM is regularly updated by the server. The tool requires user to choose a file to encrypt through user provided phrase (key). Then on demand, it uploads the encrypted data to the SSP and vice versa.

4.3 Encryption/Decryption Tool

We have developed an encryption/decryption tool which works in the browser at application layer. This tool is developed in HTML5and JavaScript. The tool used AES256 to encrypt and decrypt data. Then user's identity will be confirmed through his certificate with ACM. If the user is a valid user, the access to SSP is granted after confirming the validation of the user and his/her certificate. After that the user can download or upload his encrypted data over cloud. The client should know answers to the seven safety questions prior to making the selection of cloud providers. The data life cycle passes through seven phases: data generation, transfer, use, share, storage, archival and destruction. The tool asked from user to choose a file to encrypt through user provided phrase (key). Then on demand upload the encrypted data to the SSP and vice versa. The encryption/decryption tool has following three parts:

- ***Index.html***: This is the main file which interacts between users and server for file encryption/decryption over the network.
- ***JavaScript***
- ***CSS file***

4.4 Web Server

The web server has been built locally to provide the web services and host the encryption tool. These pages will be load the on the user browser. The tool will execute the code on user browser at client end. It is pertinent to mention that PKI used TLS/SSL protocols and encrypted communication. So, in our model encryption on the fly take place and makes very difficult for eavesdropper to read the data.

5. Experimentations

To validate our model, we installed VMWare 9.0 and built a test environment for testing and validation of our model. We have installed two Windows server 2003. One was configured to provide CA Server while the other one as web server. Then we have created three XP users (user1, user2 and user3) and made necessary network related configuration and test its communication. Here it is pertinent to mention that we are outsourcing cloud storage services for our model. Now user1 wants to store its encrypted data in cloud. First of all he required to authenticate itself as legitimate user. User1 sent request to CA server to obtain its certificate. CA server issued a certificate and updates its ACM list. Then the CA server sent the updated ACM list to SSP. After successful authentication and authorization a secure communication link established and our encrypted tool loaded User1 browser as shown in Figure 2.

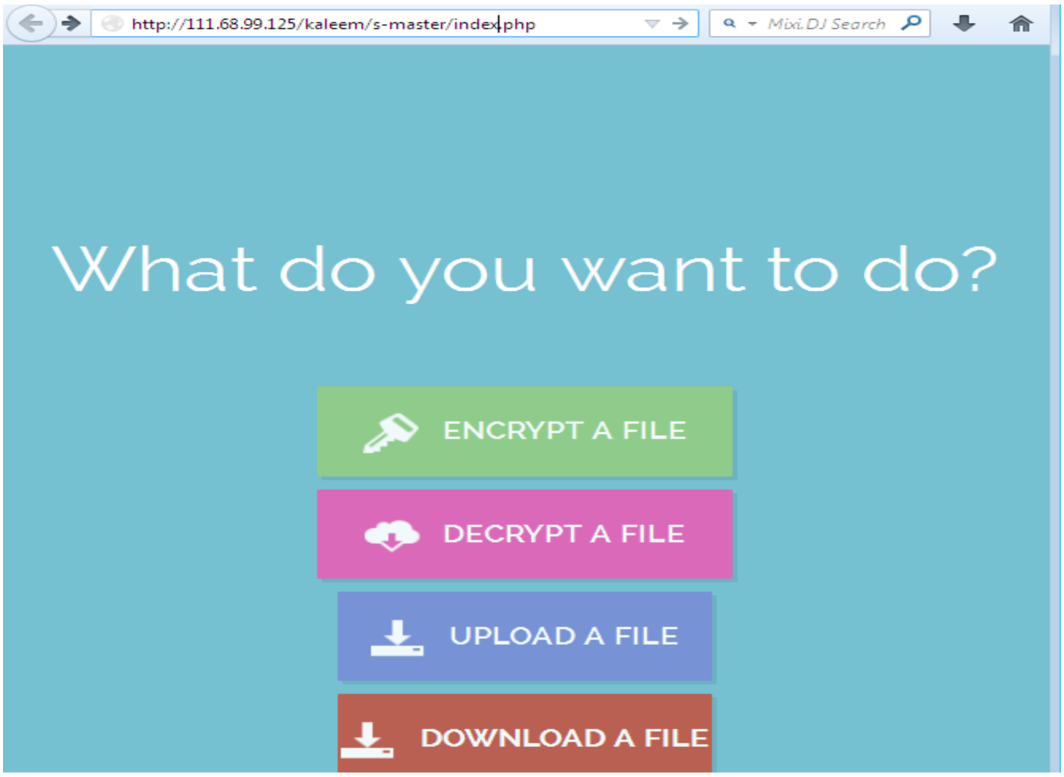

Figure 2. User Interface for the Model

User 1 encrypt his required file through a phrase (key) and save this encrypted file in its drive and then upload it to the SSP. The same can be done in reverse as User1 first download its encrypted file from SSP. And then by using our tool he will decrypt the file. Thus, in this way we have successfully tested our model. Some issues related to the model are:

5.1 The 1MB limit

There is a limitation in the system as the application does not encrypt files whose size bigger than 1MB. We have put this limit intentionally here. Because the download attribute of HTML5 does not perform better with large amounts of data. This attribute is we utilized here to suggest the encrypted file for download. Otherwise it would result in crashing the web browser particularly the Chrome and the Mozilla Firefox browsers.

5.2 What about HTTPS?

Users logically suppose the page to be loaded with HTTPS when it approaches to encrypting data and securing information. In our scenario, we believe that doing as expected by the users is not necessary, as apart from the preliminary download of the HTML and related relic, no kind of data is moved among the user and the server. Because everything is going to be happened at the client-side with JavaScript (CryptoJS).

5.3 How Secure is It?

The library that we have used is CryptoJS which is an open source; therefore, we believe it to be trustworthy. We have used the AES algorithm from the collection of libraries in the JavaScript which is generally known to be secure. For better results, it is recommended to use a long password phrase which is difficult to guess through social engineering techniques.

6. Conclusion

The objective of this study is to propose a model to address data security and privacy issues like data confidentiality and authentication in cloud computing paradigm. The cloud technology is advancing rapidly and the organizations are 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. The Chief Information Officers (CIOs) and Chief Security Officers (CSOs) of the cloud user and provider need to comprehend and address the risk and security issues in detail before actually benefitting its high-end computing power. Data security is the major concern from user point of view over cloud. One of the best ways is to always keep and transmit encrypted data in cloud. Therefore, what we have proposed to make data more secure to achieve security. Despite the limitation of software support for large files it can be widely used by enterprises. The application of the above model can be beneficiary for different branch offices of an enterprise who wants to store their sensitive data over cloud. In future we will extend our model to get integrity of the encrypted data and enhance the capability of the tool to encrypt large files.

References

[1] N. Leavitt, “Is Cloud Computing Really Ready for PrimeTime?”, IEEE Computer, January **(2009)**.

[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, 7 Oct **(2009).**

[3] H. Kharche, D. S. Chouhan, “Building Trust in Cloud Using Public Key Infrastructure”, (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 3, **(2012)**.

[4] H. kharche, Prof. D.S. Chouhan “Implementing Trust in Cloud Using Public Key Infrastructure”, International Journal of Engineering Inventions, vol. 1, issue 5, Sept. **(2012)** pp. 41-46.

[5] Y. Yang, Y. Zhang “A Generic Scheme for Secure Data Sharing in Cloud”, 2011 International Conference on Parallel Processing Workshops, **(2011)** IEEE.

[6] A.K. Dubey, A.k.Dubey, M.Namdev, S.S. Shrivastava “Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attention and sharing in Java Environment.

[7] W. A. Jansen, “Cloud Hooks: Security and Privacy Issues in Cloud Computing”, *44th Hawaii International Conference on System Sciences - 2011, IEEE.*

[8] K. Julisch and M. Hall, “Security and Control in the Cloud”, Information Security Journal: A Global Perspective, vol. 19, **(2010)**, pp. 2099-309.

[9] 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.

[10] Z. Mehmood, “Data Location and Security Issues in Cloud Computing”, International Conference on Emerging Intelligent Data and Web technologies, 2011, IEEE.

[11] D. Svantesson, R. Clarke, “Privacy and Consumer Risks in Cloud Computing”, Computer Law and Security Review, vol. 26, **(2010)**, pp. 391-397.

[12] S. A. Almulla, C. Y. Yeun, (2010, March). Cloud computing security management. In *Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on* pp. 1-7. IEEE.

[13] D. Relly, C. Wren, T. Berry, “Cloud Computing: Pros and Cons for Computer Forensic Investigations”, International Journal Multimedia and image Processing (IJMIP), vol. 1, issue 1, March **(2011)**, pp. 26-34.

[14] D. H. Patil, R. R. Bhavsar, A. S. Thorve, “Data Security over Cloud”, International Journal of Computer Applications® (IJCA), **(2012)**.

[15] S. P. Mirashe, N. V. Kalyankr, “Cloud Computing” Journal of Computing, vol.2, issue 3

[16] 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),**

[17] D. Chen, H. Zhao, “Data Security and Privacy Protection Issues in Cloud Computing”, **(2012)** *International Conference on Computer Science and Electronics Engineering, IEEE*

[18] B. R. Kandukuri, R. Paturi V, Dr. A. Rakshit, “Cloud Security Issues”, **(2009)** IEEE *International Conference on Services Computing, IEEE*

[19] Steiner, M., Tsudik, G., & Waidner, M., “Diffie-Hellman key distribution extended to group communication”, In *Proceedings of the 3rd ACM conference on Computer and communications security* , **(1996)** Jan, pp. 31-37, ACM.

[20] Iqbal S., Khalid M., Khan, M N A. "A Distinctive Suite of Performance Metrics for Software Design", International Journal of Software Engineering & Its Applications, vol. 7, no.5, **(2013)**.

[21] Iqbal S., Khan M.N.A., "Yet another Set of Requirement Metrics for Software Projects", International Journal of Software Engineering & Its Applications, vol. 6, no. 1, **(2012).**

[22] Faizan M., Ulhaq S., Khan M N A., "Defect Prevention and Process Improvement Methodology for Outsourced Software Projects", Middle-East Journal of Scientific Research, vol. 19, no.5, **(2014)**, pp. 674-682.

[23] Faizan M., Khan M NA., Ulhaq S, "Contemporary Trends in Defect Prevention: A Survey Report", International Journal of Modern Education & Computer Science, vol. 4, no. 3, **(2012).**

[24] Khan K., Khan A., Aamir M., Khan M N A., "Quality Assurance Assessment in Global Software Development", World Applied Sciences Journal, vol. 24, no. 11, **(2013)**.

[25] Amir M., Khan K., Khan A., Khan M N A., "An Appraisal of Agile Software Development Process", International Journal of Advanced Science & Technology, 58, **(2013).**

[26] Khan, M., & Khan, M. N. A. "Exploring Query Optimization Techniques in Relational Databases", International Journal of Database Theory & Application, vol. 6, no. 3. **(2013).**

[27] Khan, MNA., Khalid M., ulHaq S., "Review of Requirements Management Issues in Software Development", International Journal of Modern Education & Computer Science, vol. 5, no. 1, **(2013)**.

[28] Umar M., Khan, M N A., "A Framework to Separate NonFunctional Requirements for System Maintainability", Kuwait Journal of Science & Engineering, 39(1 B),**(2012)**, pp. 211- 231

[29] Umar M., Khan, M. N. A, "Analyzing Non-Functional Requirements (NFRs) for software development", In IEEE 2nd International Conference on Software Engineering and Service Science (ICSESS), **(2011)** pp. 675-678.

[30] Khan, M. N. A., Chatwin, C. R., & Young, R. C., "A framework for post-event timeline reconstruction using neural networks", digital investigation, vol. 4, no. 3, **(2007)**, pp. 146-157.

[31] Khan, M. N. A, Chatwin, C. R., & Young, R. C., "Extracting Evidence from Filesystem Activity using Bayesian Networks", International journal of Forensic computer science, 1, **(2007)**, pp. 50-63.

[32] Khan, M. N. A, "Performance analysis of Bayesian networks and neural networks in classification of file system activities", Computers & Security, vol. 31, no. 4, **(2012)**, pp. 391-401.

[33] Rafique, M., & Khan, M. N. A, "Exploring Static and Live Digital Forensics: Methods, Practices and Tools", International Journal of Scientific & Engineering Research, vol. 4, no. 10, pp. 1048-1056.

[34] Bashir, M. S., & Khan, M. N. A, "Triage in Live Digital Forensic Analysis" International journal of Forensic Computer Science 1, **(2013)**, pp. 35-44.

[35] Sarwar, A., & Khan, M. N., "A Review of Trust Aspects in Cloud Computing Security" International Journal of Cloud Computing and Services Science (IJCLOSER), vol. 2, no. 2, **(2013)** , pp. 116-122.

[36] Gondal, A. H., & Khan, M. N. A. A review of fully automated techniques for brain tumor detection from MR images. International Journal of Modern Education and Computer Science (IJMECS), vol. 5, no.2, **(2013)**, 55.

[37] Zia, A., & Khan, M. N. A., "Identifying key challenges in performance issues in cloud computing" International Journal of Modern Education and Computer Science (IJMECS), vol. 4, no. 10, **(2012)**, 59.

[38] Ur Rehman, K., & Khan, M. N. A., "The Foremost Guidelines for Achieving Higher Ranking in Search Results through Search Engine Optimization" International Journal of Advanced Science and Technology, 52, **(2013)**, pp. 101-110.

[39] Khan, M., & Khan, M. N. A., "Exploring query optimization techniques in relational databases" International Journal of Database Theory & Application, vol. 6, no. 3. **(2013)**.

[40] Shehzad, R., KHAN, M. N., & Naeem, M., "Integrating knowledge management with business intelligence processes for enhanced organizational learning" International Journal of Software Engineering and Its Applications, vol. 7, no. 2, **(2013)** , pp. 83-91.

[41] Ul Haq, S., Raza, M., Zia, A., & Khan, M. N. A. (2011), "Issues in global software development: A critical review" An Appraisal of Off-line Signature Verification Techniques 75 Copyright © 2015 MECS I.J. Modern Education and Computer Science, (**2015)**, 4, pp. 67-75 Journal of Software Engineering and Applications, vol. 4, no.10, 590.

[42] Zia, A., & Khan, M. N. A., "A Scheme to Reduce Response Time in Cloud Computing Environment", International Journal of Modern Education and Computer Science (IJMECS), vol.5, no.6, **(2013)**, pp.56.

[43] Tariq, M. & Khan, M.N.A., "The Context of Global Software Development: Challenges, Best Practices and Benefits" Information Management & Business Review, vol. 3, no. 4. **(2011)**.

[44] Shahzad, A., Hussain, M., & Khan, M. N. A., "Protecting from Zero-Day Malware Attacks" Middle-East Journal of Scientific Research, vol. 17, no. 4, **(2013),** pp. 455-464.

[45] Khan, A. A., & Khan, M., "Internet content regulation framework", International Journal of U-& EService, Science & Technology, vol. 4, no.3. **(2011)**.

[46] Kaleem Ullah, K. U., & MNA Khan, M. K. "Security and Privacy Issues in Cloud Computing Environment: A Survey Paper", International Journal of Grid and Distributed Computing, vol. 7, no. 2, **(2014)**, pp. 89-98.

[47] Abbasi, A. A., Khan, M. N. A., & Khan, S. A, "A Critical Survey of Iris Based Recognition Systems", Middle-East Journal of Scientific Research, vol. 15, no. 5, **(2013)**, pp .663- 668.

[48] Khan, M. N. A., Qureshi, S. A., & Riaz, N., "Gender classification with decision trees", Int. J. Signal Process. Image Process. Patt. Recog, 6, **(2013)**, pp. 165-176.

[49] Ali, S. S., & Khan, M. N. A. "ICT Infrastructure Framework for Microfinance Institutions and Banks in Pakistan: An Optimized Approach", International Journal of Online Marketing (IJOM), vol. 3, no. 2, **(2013)**, pp. 75-86.

[50] Mahmood, A., Ibrahim, M., & Khan, M. N. A., "Service Composition in the Context of Service Oriented Architecture", Middle East Journal of Scientific Research, vol. 15, no. 11. **(2013)**.

[51] Masood, M. A., & Khan, M. N. A. (2015). "Clustering Techniques in Bioinformatics" I.J. Modern Education and Computer Science, **(2015)**, 1, pp. 38-46.