

A Security Model for SaaS in Cloud Computing

R. Abbas¹, A. Farooq², S. Afghan³

^{1,2}Computer Science Department, UET Lahore, Pakistan

³University of Management and Technology, Lahore

¹rizwan_uetian@outlook.com

Abstract-Cloud computing is a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to handle applications. It has many service modes like Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS). In SaaS model, service providers install and activate the applications in cloud and cloud customers access the software from cloud. So, the user doesn't have the need to purchase and install a particular software on his/her machine. While using SaaS model, there are multiple security issues and problems like Data security, Data breaches, Network security, Authentication and authorization, Data integrity, Availability, Web application security and Backup which are faced by users. Many researchers minimize these security problems by putting in hard work. A large work has been done to resolve these problems but there are a lot of issues that persist and need to overcome. In this research work, we have developed a security model that improves the security of data according to the desire of the End-user. The proposed model for different data security options can be helpful to increase the data security through which trade-off between functionalities can be optimized for private and public data.

Keywords-Pay-As-You-Go Model, Cryptography, SaaS Security, Cloud Computing.

I. INTRODUCTION

Internet has been strongly involved in computing world so as to fulfill its modern requirements; it is approaching towards Cloud Computing. A set of different shared networks that use internet technologies to interconnect different networks and also present and deliver distinct computing services and resources to several users, clients, service providers, organizations, academia and business etc., sparing users heavy expenditures is called Cloud Computing.

Cloud Computing architecture provides the services of its miscellaneous associating computing resources and networks to its different users, clients, service providers, organizations, academia and businesses through its service delivery models [i]. There are four deployment models in cloud computing which are Private cloud, Public cloud, Community

cloud and Hybrid cloud. There are some service delivery models in cloud computing like Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Everything as a Service (XaaS).

SaaS is a software deployment model where applications are remotely hosted by the application or the service provider and made accessible to customers on demand, over the Internet. The SaaS model provides the customers sizable benefits, such as ameliorated operational efficiency and decreased costs. SaaS is rapidly rising as the dominant delivery model for fulfilling the necessities of enterprise IT services. However, most enterprises are still disagreeing with the SaaS model due to deficiency of visibility about the way their data is stored and secured [i].

Many researches provide different security models and contribute their efforts to resolve the security issues and problems in SaaS model but there are lots of issues that need to be overcome to improve the security level. These security issues are Data security, Data breaches, Network security, Backup, Authentication and Authorization, Web application security, Availability and Data integrity.

Our study is based on SaaS security issues aiming at Data security in this research. As it is already discussed that the SaaS is floating over PaaS and PaaS on IaaS, so in somehow the security related with SaaS is interconnected with both of underneath layers, eventually more responsible security is the security of SaaS. A high degree of integrated functionality is given by the SaaS model but minimum customer control or extensibility is presented by it. On a lower level the PaaS due to its relatively lower degree of abstraction provides relatively greater customer control and greater extensibility. More power and customer control over security is offered by IaaS, the lowest bed as compared to PaaS or SaaS [ii].

We are going to elaborate a summary of Cloud Computing infrastructure and its associated services, Issues in SaaS model and existing solutions in section 2. And we will also explain our proposed security model for SaaS and block diagrams in section 3. We will discuss a case study which justifies our proposed model with Encryption and Decryption process in section 4. Finally, we will conclude our work in section 5.

II. LITERATURE REVIEW

With the computing characteristics of cloud computing, the server deals with various issues associated with safeguarding of data which is the prime asset of the user. In [vii] M. R Faheem explains the latest issues of cloud computing connected to its services for data solidarity and web browsing etc. On security issues along with data hosting and services provided in Cloud Computing, a comprehensive study has been applied in literature [ix, iii]. The requirements of control on related threats and exposures in cloud computing is taken by generic design principles [iv].

In [v], author admires Cloud computing for its possibilities abstracted hardware, generally personalized, platform-agnostic, cheap and QoS promised etc. Our effort (attempt) of different literature studies moves our attention towards NIST definition.

The National Institute of Standards and Technology (NIST) defines Cloud Computing in its Special Publication 800-145 i.e., “*Cloud computing is a model for enabling ubiquitous, 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* [vi].”

A. Cloud Computing Infrastructure

Cloud Computing contains four deployment models and three service models.

Four deployment models are as follow:

Private Cloud

If a cloud is used by organizations that may operate on its own and manage it by itself or by a third party and it may sustain exclusive or inclusive of a premise is called private cloud.

Community Cloud

If a cloud is offered to one or more organizations colligated to a specific community that may be owned, operated and managed by the community itself or a third party it may sustain exclusive or inclusive of a premise is called community cloud.

Public Cloud

If a cloud is offered to general public that may be owned operated and managed by an organization, government or a business community or it may subsist in the provider's premise is called public cloud.

Hybrid Cloud

An integrated combination of some separate clouds i. e., two or more Private, Public and/or community clouds colligating for load balancing and efficient data portability.

Three Service Models are as follow:

Software as a Service (SaaS)

In this model cloud provider provides various kinds of Software applications on-line through internet e.g., different software, online running applications, e-mail applications, web browsing applications etc., are provided to clients using them without superseding the lower tier infrastructure.

Platform as a Service (PaaS)

This is lower layer of SaaS in which application deployment capabilities are provided to a provider. The applications developed by programming languages, libraries, services etc., can be deployed but control over lower infrastructure is restricted.

Infrastructure as a Service (IaaS)

In this model consumer provides a limited control over lower tier infrastructure like configuration setting, memory management, and network resources etc.

These service delivery models conjointly form a layered architecture as shown in Fig-1. SaaS model is the outer core of the infrastructure which enables applications servicing and it resides on PaaS layer. PaaS model is the central core of the infrastructure which enables deployments services of applications and it dwells on IaaS layer. IaaS model is the lower bed of the infrastructure which consists of the services of system, networks and hardware resources.

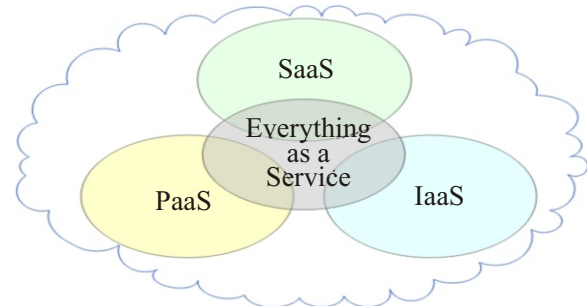


Fig. 1. Service Delivery Model of Cloud Computing

B. Security Issues of SaaS

An analysis of efforts of different authors on some security matters of Cloud Computing as vulnerabilities, warnings, procedures, security standards, data security, certainty, security requirements and SaaS, PaaS, IaaS security are issued by Hashizume et al. In [ix] our study is based on SaaS security issues aiming at Data security in this research. As it is already discussed that the SaaS is floating over PaaS and PaaS on IaaS, so in some regard the security related with SaaS is interconnected with both of underneath layers, eventually more responsible security is the security of SaaS. A high degree of integrated functionality is given by the SaaS model but minimum customer control or extensibility is presented by it. Beneath it the PaaS due to relatively

lower degree of abstraction provides relatively greater customer control and greater extensibility. Greater power or customer control over security is offered by IaaS the lowest bed as compared to PaaS or SaaS [ii].

Data is the key feature to be kept secure for almost all the users, either solitary or from an organization's platform. The user is dependent to its cloud provider in SaaS in regard of security concerns because user's data is stored in data center at provider's proximity. Certainly, other user's data is also stored there. So, there is a probability of mixing of irrelevant data with enterprise data if a SaaS provider is related with a Public Cloud Service. In addition the cloud provider might replicate the data in case to obtain high availability and rapid access of data at multiple locations on the globe. So un-awareness of placements of user's data causes the lack of control that involves an un-guaranteed situation in the SaaS model [viii].

This case may create another problem that if a user wants to remove his data, he does not know where it is stored and while trying a removal action, it is removed from all the locations where it was duplicated by provider at time of storing. Software applications and databases are moved by cloud computing services to enlarge data centers where the dependability of management services is not aspiring. This activity generates many security problems and issues [x]. The privacy of a user data from other users is the responsibility of the provider In the SaaS model.

By definition, for the cloud customer, new software applications are substituted with old ones periodically or sporadically. So for accomplishment of a successful data migration, the protection or enhancement of the security functionality (along with portability of applications) issued by the legacy application must be concentrated by the provider.

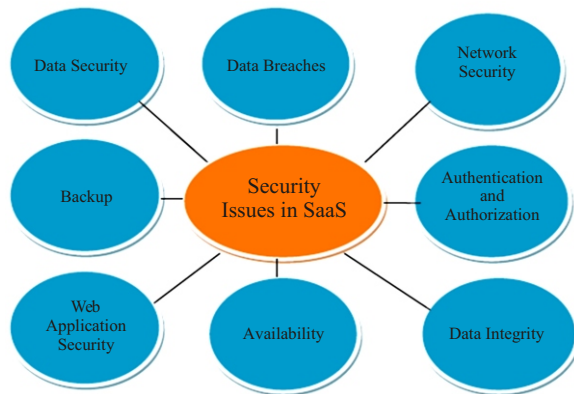


Fig. 2. Security Issues in SaaS

III. RELATED WORK

In [xi] Prashant Srivastava, et al., proposed a structural design that works as a proactive model to handle the progressively more security problems in

cloud computing. Their proactive methodology creates a detailed cloud policy and according to this policy, client identifies the suitable service provider which satisfies the client's security requirements. Security is continuously monitored by the security cloud. Inform security measures are taken by the client when there is any violation in cloud security policy

In [xii] Eman M. Mohamed, et al., introduced Enhanced Data Security Model for Cloud Computing which is divided into three layers. The first layer authenticates the user by using OTP (One-Time-Password) technique. The second layer performs encryption on user's data, and protects the user's privacy by using one symmetric encryption algorithms. Also allow protection from user. Finally, they implemented this software in the Amazon EC2 Micro instance and obtained positive results.

In [xiii] Steven Y. KO, et al., proposed a Hybr Ex (Hybrid Execution) model for securing data privacy in cloud computing. This model uses partitioning of data and computation as a way to provide confidentiality and privacy of data. Also they discuss how this model is one specific execution requirement, Map Reduce over Big table.

In [xiv] H. Raj, et al., present a resource isolation technique which enables the deployment of VMs (Virtual Machines) with isolation enhanced SLAs (Service Level Agreement). They propose to deploy many of such VMs in the ownership of different independent SPs (Service Providers) under the decisions of the RM (Resource Manager) of the CIP (cloud Infrastructure Provider). They claim about Security of data during processing.

TABLE I
PROPOSED MODEL VS PREVIOUS MODEL

Attribute	Proposed Technique	Previous Technique
Cypher length	Moderate	Bigger
Effective	More Effective	Less Affective
Complexity	Less complex	More Complex
Memory	Takes Shorter memory	More memory Required
Processing	Takes less processing	Takes more processing
Cypher	ASCII, Binary and Decimal	Usually Binary

IV. PROPOSED MODEL

In SaaS, organizational data is often processed in plain text and is stored in data center of the cloud. The main responsibility of security of the data falls on the shoulders of SaaS provider while storing data in the data center and its management as well. Our approach

to secure data is based upon making responsible both parties i.e, the user and the provider. We believe due to this approach high security of private and enterprise data will be achieved. There are three different levels of security that are available in this model. These security levels are named as level-1, level-2 and level-3. Client has the data of different nature so client's data can be secure with different level of security based on the

desire of client. Level-1 is lowest and level-3 is highest security level.

In level-1, client simply authenticates by password and stores the data on the behalf of service provider's security technique. In level-2, client encrypts data by using algorithm-1 technique. In level-3, client secures his/her most private data by using algorithm-2 method and then sends to service provider.

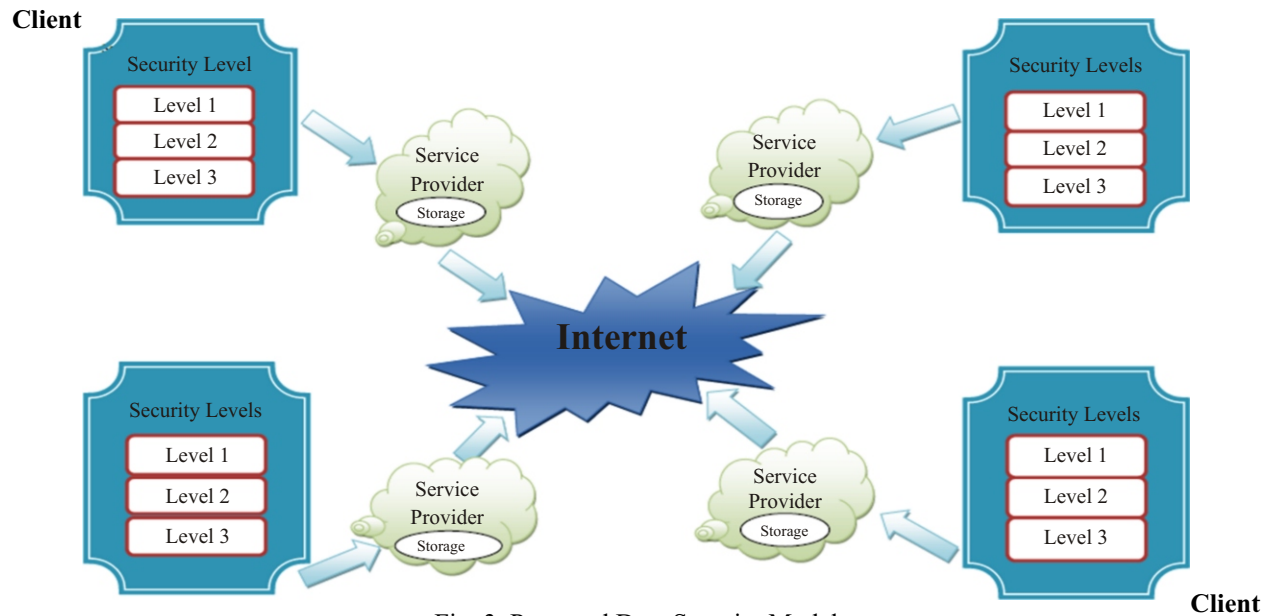


Fig. 3. Proposed Data Security Model

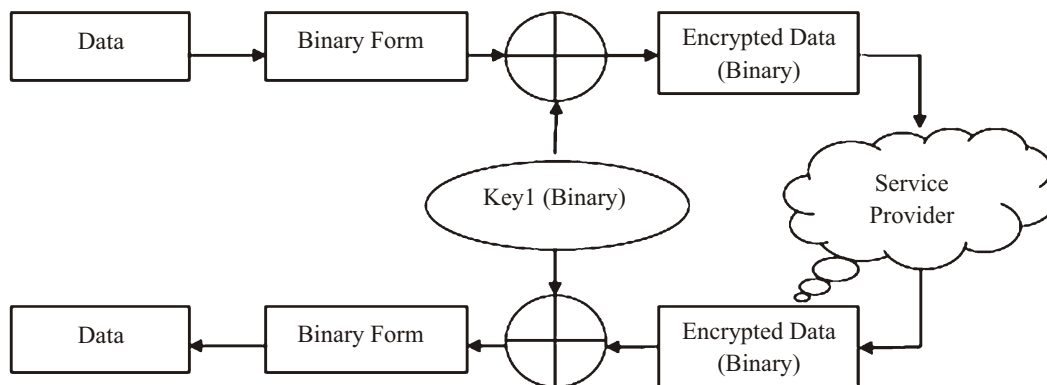


Fig. 4. Block Diagram of security level-2

Level-2 (Encryption)

Step 1. "Convert data into Binary form by using ASCII values."

For letter "H" its ASCII value is "72" and Binary form of "72" is "01001000"

Step 2. "Select the binary key"

It can be any 4-digit binary key which repeats two times while performing operation on 8-digit binary value. Here, binary key is "1010".

Level-2 (Decryption)

Step 1. "Select the binary key"

Key is same which is used for encryption that is "1010".

Step 2. "Perform XOR operation on binary data by using selected key"

Binary encrypted data is "11100010" and key is "10101010". After taking XOR operation output value is "01001000".

Step 3. “Perform XOR operation on binary data by using selected key”

Binary converted data is “01001000” and binary key is “10101010”. After taking XOR operation output binary data is “11100010”.

“11100010” is the output encrypted binary data.

Step 3. “Convert Binary form into original data by using ASCII values.”

For binary value “01001000”, its ASCII value is “72” which is equal to alphabet “H”.

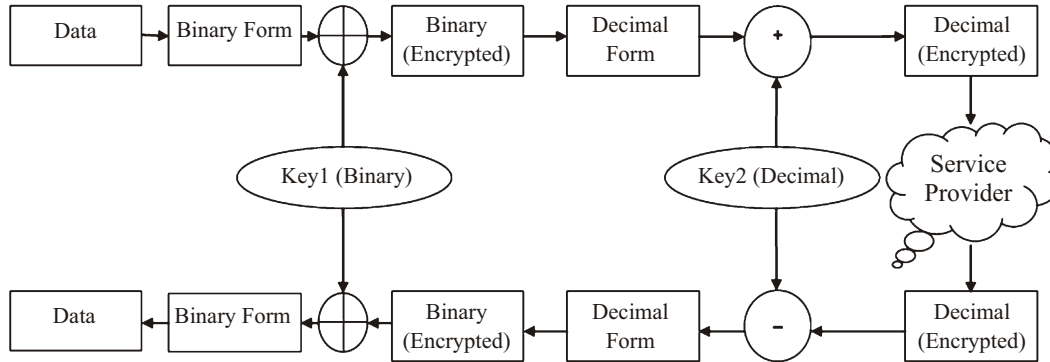


Fig. 5. Block Diagram of level-3 security

Level-3(Encryption)

Step 1. “Convert data into Binary form by using ASCII values.”

For letter “H” its ASCII value is “72” and Binary form of “72” is “01001000”

Step 2. “Select the binary key”

It can be any 4-digit binary key which repeats two times while performing operation on 8-digit binary value. Here, binary key is “1010”.

Step 3. “Perform XOR operation on binary data by using selected key”

Binary converted data is “01001000” and binary key is “10101010”. After taking XOR operation output binary data is “11100010”.

“11100010” is the output encrypted binary data.

Step 4. “Convert binary encrypted data into Decimal form”

Decimal form of binary encrypted value “11100010” is “226”.

Step 5. “Select the decimal key”

It can be any decimal value so here we take “323” as a decimal key.

Step 6. “Perform Addition operation on decimal data by using selected decimal key”

Decimal converted value is “226” and decimal key is “323”. After taking addition operation output decimal data is “549”.

“549” is the output encrypted decimal data.

“323”.

Step 2. “Perform Subtract operation on decimal data by using selected key”

Decimal encrypted data is “549” and key is “323”. After performing subtraction operation output value is “226”.

Step 3. “Convert decimal data into binary form”

Binary form of decimal value “226” is “11100010”.

Step 4. “Select the binary key”

Key is same which is used for encryption that is “1010”.

Step 5. “Perform XOR operation on binary data by using selected key”

Binary encrypted data is “11100010” and key is “10101010”. After taking XOR operation output value is “01001000”.

Step 6. “Convert Binary form into original data by using ASCII values.”

For binary value “01001000”, its ASCII value is “72” which is equal to alphabet “H”.

V. CASE STUDY

In this case study, we perform Encryption and Decryption process for Level-2 and Level-3 security by following algorithm-1 and algorithm-2 respectively and compare the results.

The original Data is “HELLO”

Level-3 (Decryption)

Step 1. “Select the decimal key”

Key is same which is used for encryption that is

Level-2**(Encryption Process)****“Data = HELLO”**TABLE II
LEVEL-2 ENCRYPTION FOR “HELLO”

Character	ASCII	Binary	Key1	XOR Operation
H	72	1001000	1010	11100010
E	69	1000101	1010	11101111
L	76	1001100	1010	11100110
L	76	1001100	1010	11100110
O	79	1001111	1010	11100101

**“Encrypted data =
1110001011101111111001101110011011100101”****(Decryption Process)****“Encrypted data =
1110001011101111111001101110011011100101”**TABLE III
LEVEL-2 DECRYPTION FOR “HELLO”

Encrypted Data	Key1	XOR Operation	ASCII	Data
11100010	1010	1001000	72	H
11101111	1010	1000101	69	E
11100110	1010	1001100	76	L
11100110	1010	1001100	76	L
11100101	1010	1001111	79	O

“Data = HELLO”**Level-3****(Encryption Process)****“Data = HELLO”**TABLE IV:
LEVEL-3 ENCRYPTION FOR “HELLO”

Data	ASCII	Binary	Key 1	XOR	Decimal	Key 2(k2)	(k2+D)
H	72	1001000	1010	11100010	226	323	549
E	69	1000101	1010	11101111	239	323	562
L	76	1001100	1010	11100110	230	323	553
L	76	1001100	1010	11100110	230	323	553
O	79	1001111	1010	11100101	229	323	552

“Encrypted Data = 549562553553552”**(Decryption Process)****“Encrypted Data = 549562553553552”**TABLE V
LEVEL-3 ENCRYPTION FOR “HELLO”

Enc. Data	Key 2(k2)	Decimal	XOR	Key 1	Binary	ASCII	Data
549	323	226	11100010	1010	1001000	72	H
562	323	239	11101111	1010	1000101	69	E
553	323	230	11100110	1010	1001100	76	L
553	323	230	11100110	1010	1001100	76	L
552	323	229	11100101	1010	1001111	79	O

“Data = HELLO”

VI. RESULTS

Here, we discuss the favorable factors of proposed model as compare to previous security models as we mention in Table I.

Effective: There are number of security models which are used to encrypt data but the techniques used by these models require lot of processing, memory and also complex algorithms. The proposed technique also performs cryptography but it requires less processing, less memory and easy steps to perform encryption. Therefore, the proposed security model is more effective as compare to previous security models.

Complexity: In this proposed model, each level (2, 3) uses only two keys to encrypt the plain text. These keys use binary and decimal languages which are easy to understand for machine as well as human. Due to these simple and effective keys the proposed technique is less complex as compare to previous security models.

Memory: The level-3 converts the binary data which is the result after binary key encryption into decimal digits. The decimal digits need less memory for storage as compare to other languages which is used in old security models. Therefore the encrypted data of proposed model consumes less memory as compare to previous models.

Processing: The proposed model only performs XOR operation on binary and decimal data for data encryption. XOR operation is the basic operation which is easy to process for machine. So, the proposed technique requires less processing as compare to previous models.

VII. CONCLUSION

Although cloud computing is a versatile environment of heterogeneous and distributed networks which provides services to several customers and enterprises to share heterogeneous networks, resources and software online using internet technologies. In this work we have concluded that numerous threats of security and vulnerabilities have been arisen with the development and advancement in such a complex, huge meshed, word-wide distributed infrastructure. Till now many researchers have contributed to secure the users from these issues by providing different techniques, encryption and signatures etc., but complexities increases due to the tradeoff between different issues and functionalities inherited in this domain. In this paper, we proposed a security model which has three different levels and each level has its own algorithm. Client has data of different types so client can secure data according to required security level.

In our Future Work we are focusing to work for a flexible model of services which can offer an optimum situation for the availability of encrypted data i.e.,

lower-level of trade-off between security functionality and availability.

REFERENCES

- [i] A. A. Soofi, "Security Issues in SaaS Delivery Model of Cloud Computing", *International Journal of Computer Science and Mobile Computing*, ISSN 2320-088X, Vol.3, Issue.3, pg. 15-21, March 2014.
- [ii] Cong, "Ensuring data storage security in Cloud Computing", in *IWQoS 2009, 17th International Workshop on Quality of Service*, pp. 1-9, 2009.
- [iii] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*, vol. 34, pp. 1-11, 2011.
- [iv] D. Zissis and D. Lekkas, "Addressing cloud computing security issues ", *Future generation Computer Systems*, Elsevier, 28 (2012) 583-592, 2012.
- [v] S. V. Nandgaonkar and A. B. Raut, "A Comprehensive study on Cloud Computing", *International Journal of Computer Science and Mobile Computing*, ISSN 2320-088X, Vol.3, Issue.4, pg. 733-738, April 2014.
- [vi] NIST SP 800-145, —ANIST definition of cloud computing, 2012, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (Accessed: January 2015).
- [vii] M. R. Faheem, "Security Issues of Cloud Computing", *International SAMANM Journal of Business and Social Sciences*, ISSN 2308-2372, Vol. 2, No. 3, July 2014.
- [viii] T. Mather, K. Swamy and Latif, "Cloud Security and Privacy", O'Reilly Media, Inc., Sebastopol, CA, 2009.
- [ix] Hashizume, "An analysis of Security Issues for Cloud Computing", *Journal of Internet Services and Applications*, Springer Open Journal, 2013, 4:5.
- [x] A. Seccombe, H. Alex, A. Meisel, A. Windel, A. Mohammed, A. Licciardi, "Security guidance for critical areas of focus in cloud computing", *Cloud Security Alliance v2.1*, 25 p, 2009.
- [xi] P. Srivastava, "An architecture based on proactive model for security in cloud computing", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 MIT, Anna University, Chennai. June 3-5 2011.
- [xii] E. M. Mohamed, "Enhanced Data Security Model for Cloud Computing", the 8th International Conference on Informatics and Systems (INFOS2012), Cloud and Mobile Computing Track, 14-16 May 2012.
- [xiii] S. Y. Ko, K. Jeon, and R. Morales, "The HybrEx

model for confidentiality and privacy in cloud computing," in Proc. of Hot Cloud, 2011.
 [xiv] H. Raj, R. Nathuji, A. Singh, and P. England. Resource management for isolation enhanced

cloud services. In ACM Cloud Computing Security Workshop, pages 77-84, November 2009

Authorship and Contribution Declaration			
	Author-s Full Name	Contribution to Paper	
1	Mr./Dr./Prof. Alpha (Rizwan Abbas)	Proposed topic, basic study Design, methodology and manuscript writing	
2	Mr./Dr./Prof. Bravo (Dr. Amjad Farooq)	Data Collection, statistical analysis and interpretation of results etc.	
3	Mr./Dr./Prof. Charlie (Sher Afghan)	Literature review & Referencing and quality insurer	