DIAGNOSIS SECURITY PROBLEMS IN CLOUD COMPUTING FOR BUSINESS CLOUD

[1,2] **MOHANAAD SHAKIR,** [2] **ASMIDAR BIT ABUBAKAR,** [2]**YOUNUS BIN YOUSOFF,**
[3]**ALI MAKKI SAGHER ,** [1]**HUSSAM AlKAYALI**

[1]Alburaimi University Collage(BUC), Oman, [2]University Tenaga National(UNITEN) , Malaysia
[3]Univesity of Alanbar, Iraq

E-mail: [1]mohanaad@buc.edu.om , [2]asmidar@uniten.edu.my,[3]Yunusy@uniten.edu.my,
[3]ali_makki@uoanbar.edu.iq , [4]hussam@buc.edu.om

ABSTRACT

Cloud computing is considered as one of the rapid growing technologies for it has high flexibility in both usage and application; therefore, it has been used widely by many organizations. Cloud computing features ease, fast accessibility of the data and cost reduction for data storage. Consequently, a number of organizations are using this technology. Since the cloud computing has been used widely in various parts of the world by many originations, several security problems in cloud computing exist. This study was carried out by distributing questionnaires to different organizations in selected twelve (12) countries. This paper aims to examine the security problems and to identify the characteristics of such security problems, in addition this study will examine the important issues in security cloud computing and will determine the frames to improve security systems for cloud computing. The findings of this study, firstly   the organizations or institutions are very concerned in improving the security of cloud computing through the application of the authority model and dynamic classification of data model based on the multi-level security. Secondly , they prefer to develop the multi-key cipher algorithm in order to manage the encryption based on the level of security .

Keywords: *Information system security, Cloud computing, AES, Data classification .*

1. INTRODUCTION

Cloud Computing has recently introduced a computing model. Its main advantages lie in upgrading hardware power efficiency and use of resources. At the same time, it gives users the opportunity for universal access and provides them the privilege to reimburse the services they have received. Cloud computing is defined in multiple ways due to its relatively young presence. However, in this current study, we follow NIST's definition, which states that Cloud Computing is "a model for enabling convenient, on-demand network access to a shared pool 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" [1]. The essence of Cloud Computing extends to a wide range of information, software, and resources that are made available to the consumers through their very own browsers.

Cloud Computing has used insights from other computing software and paradigms like Web 2.0 and virtualization SOA (Service Oriented Architecture). To some extent, Cloud Computing can be considered as a result of these paradigm evolution, and so the name itself stands for the change they have undergone with respect to the service they stand for [2]. Cloud Computing can be used in one of its three model variations as shown in figure 1 below, namely PaaS (Platform-as-a-Service), IaaS (infrastructure-as-a-Service), and SaaS (Software-as-a-Service). PaaS involves the utilisation of platform layer resources like operating system abutment and software frameworks. It introduces, expands or transfers the resources to the cloud. On the other hand, IaaS is the most basic-resource provider, which deals with networks, storage, and processing, ensuring that the consumer is able to optimise random software, applications, and operating systems. Moreover, SaaS is the final model which gives the customer the option to choose from a wide range of cloud-implemented, end-user applications, which are brought to the consumer through a thin interface (for example, web-based e-mail) to their preferred device. Cloud computing, undoubtedly presents multiple advantages, but its limitations, including legal issues, security, standardization and privacy, must be kept in mind. Every model comes with certain

security complications. In addition to its own security problems, it has still not overcome the ones inherited by the technologies it has been influenced by or which have acted as its fundamental bases, which impedes system security performance even more. Although many security measures have been taken with respect to singular system parts, there is no unified system for protecting the whole cloud. This is precisely where we have concentrated our efforts – in the procurement of a general system for handling system security concerns.
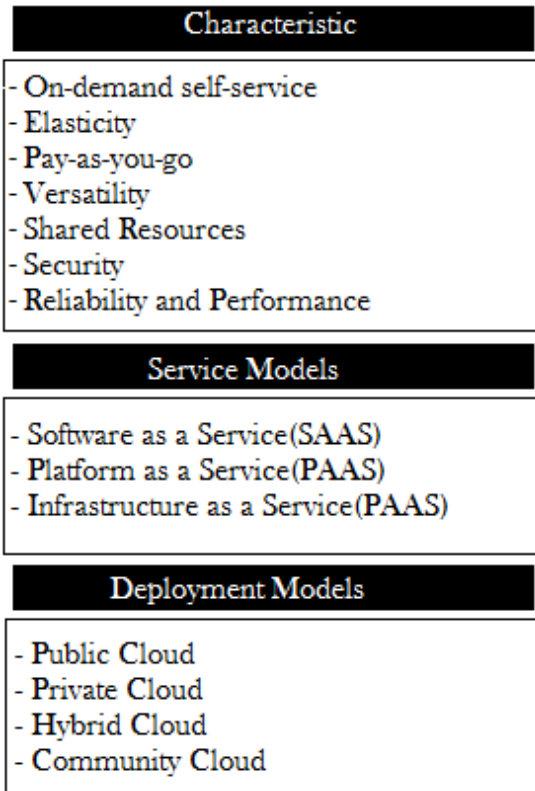
Characteristic

- On-demand self-service
- Elasticity
- Pay-as-you-go
- Versatility
- Shared Resources
- Security
- Reliability and Performance

Service Models

- Software as a Service(SAAS)
- Platform as a Service(PAAS)
- Infrastructure as a Service(PAAS)

Deployment Models

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

Figure 1 Cloud Computing layers

2. SECURITY AND PRIVACY REQUIREMENT

Security deals with information privacy, integrity and availability, and is additionally characterized by AAA (Researcher Authorization, Authentication, Access control), as shown in figure 2 below.

Figure 2. AAA Triangle

Privacy, in turn, relates to the adherence to certain legal and functional requirements, including client agreement, personal identification and legitimate usage, and security constraints. Moreover, it is controlled, it complies the privacy in cloud computing and it is clear in its policy. When these requirements are met, the cloud arrangement is considered to be lawfully operated. ISO 7498 2 imposed by the International Standards Organization concerns some supplementary specifications:

Confidentiality, Identification and Authentication management, *Researcher station and access, Integrity*, *Availability, Compliance and Audit, Transparency*, *Governance, Accountability.*

Confidentiality involves the numerous cloud access points and users, which makes it sensitive to illegitimate venues and pirate individuals. It ensures that only authorized users can access their data. It is also mandatory to maintain confidentiality for public clouds since they are most vulnerable to security threats. Software applications, shared information and profiles, information exposure, and weak user identifications are among the immediate threats concerning the cloud storage [22]. The cloud's multitenancy characteristics pose a threat to user data abuse since resource sharing among clients can expose the private information. This is largely due to the fact that a cloud separates its data assets virtually. Information that has been deleted can be retained and reconstructed because the cloud's data remnants can be retrieved by anyone using various softwares. Consequently, the data can be stolen, changed or copied. Therefore, fraud protection should be implemented because weak security may result to an illegitimate data access. It is mandatory that cloud service providers must protect the users from breaches coming from various software applications, which require access to the clients' information [16]. Data in cloud computing must remain secure and unavailable to third parties. In fact, privacy of the data can be secured through the use of popular techniques like 2FA [18, 17] and encryption algorithms [20, 19].

3. SECURITY RISKS IN CLOUD:

Gardener describes seven popular security risks [23] that clients should tackle with vendors before a cloud computing system is chosen [24] as show in figure 3 below.

- Privileged user access.
- Regulatory compliance.
- Data location.
- Data segregation.
- Recovery.
- Investigative support.
-Long term viability.

Figure 3 SECURITY RISKS IN CLOUD

First is privileged user access, which has to do with the personnel who can maintain and access your data. Clients must ask the CSP about hiring practices and the people responsible for such process. Second is regulatory compliance, and this has to do with regular external audits and certifications for security. Third is data location. It is highly possible that your data may be processed and maintained in a different country, and you may not know it. In some countries, restrictions are applied to the transfer of data overseas. In addition, virtualisation technologies hinder the identification of data location, such that CSPs must follows local privacy requirements to safeguard the privacy of data. Fourth is data segregation. This stands for the division or categorisation of data so that cloud clients could only access certain information without affecting that of others. CSPs should hire security to perform this. Fifth is data recovery, which is important in terms of retrieving data in the case of calamities or unforeseeable circumstances. The CSP must be able to ensure that storage media are reliable and that the data may be recovered to the fullest extent. Sixth is investigative support, which has to do with the measures in place to monitor any illegal activity that may be occurring on the cloud. The last one is long-term viability. What this means is that a CSP has the capability to make the data available for the long term, as long as necessary, even when no longer in operation. Carrol et al. [25] outlined a number of control objectives that are important in terms of addressing security risks in the cloud. These objectives include administration and control, data security, network security, physical security, logical access, compliance, and virtualisation. The risks that can be associated with these objectives were described, and recommendations for mitigating risk were given. Tanimto et al. [26] proposed the breakdown structure (RBS) for risk identification. The identified risks could be analysed and assessed with the use of the risk matrix method, which categorises risks based on the frequency of generation and the degree of incidence. Four countermeasures are determined, namely risk mitigation through the reduction of its effect to an acceptable degree, risk transference to a third party, risk avoidance alternatives, and unconditional acceptance.

4. OBJEVTEVES

The objectives of this study are:

- To examine the security problems and to identify the characteristics of such security problems;
- To examine the important issues in security cloud computing and determine the frames to improve security systems for cloud computing.

5. METHODOLOGY

In this paper, we diagnosed the problems of security in cloud computing. Cloud computing has faced many problems in security which includes cipher, information hiding, information security, intruder and others. Therefore, the use of cloud computing in organizations or institutions may pose a number of security problems. To determine these problems, we firstly conducted a survey to various organizations that use the cloud computing. The questionnaires were distributed to collect the required data in order to diagnose the problems in security of cloud computing and to define the nature of these problems. The collected data gave a clear understanding about the existing problem and the method on how to address the issue in multi security problems with cloud computing. The total number of samples collected was fifty six (56) cases in twelve (12) selected countries. The survey was disseminated through the website. Moerover, observation was also conducted in many organizations that used the cloud computing, such as universities, company, and government institutions. In addition, the data were analyzed using a statistical analysis to find out the problems that the organization faces.

This study hopes to shed light on the common problems of cloud computing security particularly in maintaining confidentiality of the data. Figure 2 shows the steps of the methodology.
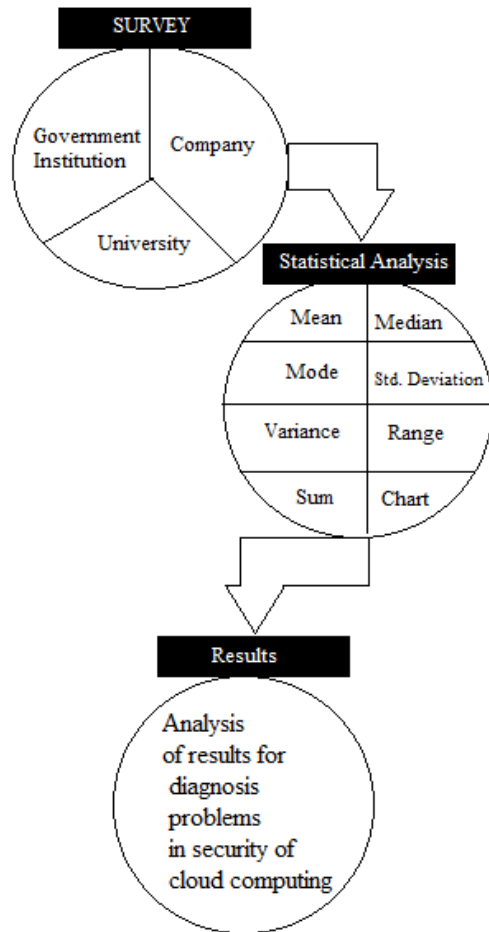
Fig. 4. Methodological Framework

6. PARTICIPANTS

The participants of this study were organizations that use the cloud computing. This study focused on the experts as participants such as Professor, Lecturer, IT Professionals and researchers who had interests in security in cloud computing. In this study, organizations from twelve (12) countries (as shown in Table 1) were selected to ensure a wider scope of data collection which helped to diagnose the problems that were identified. The total number of the data collected was one hundred twenty five (125), however, only fifty six (56) were chosen from various organizations because the focus of the study was on the experts who used the cloud computing. Based on the results of this survey, it is found that most of the organizations that used cloud computing suffered from security problems.

7. DATA COLLECTION INSTRUMENT

This research consists of two phases of data collection. The first phase includes the background information of the participants and organizations while the second phase focuses on the cloud computing security. The data collection was conducted by distributing the questionnaire and collecting the feedback from various organizations via email and field visits within a period of six months. However, the organizations that did not use cloud computing were not included as part of the data of this study.

Table 1 shows the data collected on the background information of the participants and organizations. It shows that 10 participants have Doctorate degree, 22 of them have Master's degree, 21 of them have Bachelor's degree, 2 Associate degree and one high school graduate. The table (Table 1) also presents the age, location, position and years of experience of the participants.

On the other hand, the second part (Part 2) of the questionnaire focuses on the confidentiality of cloud computing.

Table 1. Questionnaire distribution

Part 1					
Q1:	*Title of qualification awarded*				
High School		**Asst. degree**	**Bsc**	**Msc**	**PhD**
1		2	21	22	10
Q2:	*Age*				
20-25	**25-30**	**30-35**	**35-40**	**40-50**	**Over 50**
2	12	14	16	10	2
Q3:	*Location*				
Iraq	**USA**	**KSA**	**Jordan**		**Turkey**
10	7	3	2		5
UAE	**Canada**	**Australia**	**Malaysia**		**India**
3	3	7	9		2
Oman		**Germany**			
2		3			
Q4:	*Position*				
Managing Director		**Manager**		**Academic staff**	
4		6		20	
IT Professional		**Programmer**		**Others**	
16		8		2	
Q5:	*Years of experience in the aforementioned position*				
0-2	**2-5**	**5-10**	**Over 10**		
0	2	35	19		
Q6:	*Work sector*				
Insurance	**Education**		**Bank**	**Computer/ IT**	
4	27		3	8	
Government agencies		**Healthcare**		**Other**	
7		6		1	
Q7:	*Number of staff OR student at your organization*				
0 till 100			**101till 299**		

9	21
300 till 599	**Over 600**
22	4

Part 2: Confidentiality

1:	I am concerned with the improvement features of security in cloud computing.

Strongly Agree	*Agree*	*Neither*	*Disagree*

2:	I often face problems in the authority model of cloud computing.

Strongly Agree	*Agree*	*Neither*	*Disagree*

3:	I prefer the authority of cloud computing that has Multi-level security.

Strongly Agree	*Agree*	*Neither*	*Disagree*

4:	Data differ based on the level of security in the cloud computing.

Strongly Agree	*Agree*	*Neither*	*Disagree*

5:	Data need various sizes of key encryption according to the level of security.

Strongly Agree	*Agree*	*Neither*	*Disagree*

6:	Timing of encryption and decryption is vital.

Strongly Agree	*Agree*	*Neither*	*Disagree*

7:	The legality of data which upload on cloud computing is important.

Strongly Agree	*Agree*	*Neither*	*Disagree*

8:	I prefer the process of recognizing and notifying the illegal data.

Strongly Agree	*Agree*	*Neither*	*Disagree*

8. DATA ANALYSIS AND RESULTS

The statistical analysis and evaluation of the data in this study were done by using Mean, Median, Mode, Std. Deviation, Variance, Range, and Sum. SPSS was used for statistical relation analysis and Excel for Statistical graphic summary as shown in Fig. 4 (statistical analysis).

The triple averages include Mean, median, and mode. However, there are many types of averages in statistics and one of those "averages" is the "mean" and the "median" which is the mid value. The recurring values are called "mode" [13]. Std. Deviation is a statistical dimension or appraise of the dispersion of a set of data from its mean. The more spread the data is, the higher is the deviation. Standard deviation is calculated as the square root of variance [14].

The variance is the measure of the spreading set of data that points around their mean value. Variance is a mathematical prospect of the average squared divergences from the mean [15].
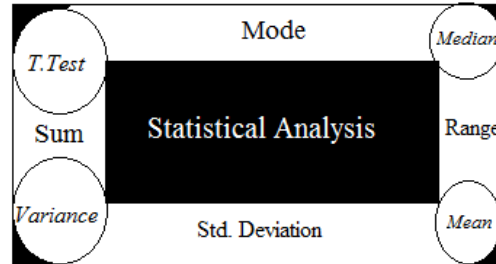

Figure 4. Statistical Analysis

Range is one of the several indices of inconsistency that statisticians use to characterize the dispersion among the measures as given in samples [21]. Below is an explanation of the analysis for Part 2.

Table 2. Descriptive Statistics Part 2

	N	R	M ni	Maxi mum	Sum	Mean
	Statistic					Std. Error
Q1	**56**	3.0	1.0	4	92.0	1.6429	.13100
Q5	**56**	2.0	1.0	4	74.0	1.3214	.07256
Q2	**56**	3.0	1.0	4	80.0	1.4286	.12183
Q3	**56**	2.0	1.0	3	72.0	1.2857	.07942
Q4	**56**	2.0	1.0	3	72.0	1.2857	.07942
Q6	**56**	2.0	1.0	3	71.0	1.2679	.07425
Q7	**56**	2.0	1.0	3	66.0	1.1786	.05759
Q8	**56**	2.0	1.0	3	66.0	1.1786	.06297
Val	56						

	Std. Deviation	Variance
	Statistic	Statistic
Q1	.98033	.961
Q5	.54296	.295
Q2	.91168	.831
Q3	.59435	.353
Q4	.59435	.353
Q6	.55567	.309
Q7	.43095	.186
Q8	.47125	.222
Valid N (listwise)		

Table 2 shows the results of the survey questionnaire that was distributed to the participants. The findings reveal the mean of each question in the survey. Question 1 (Q1) has a mean score of 1.6429 and Q8 has a mean score of 1.1786.

Detailed analysis of the data is further discussed in Table 3.

Table 3. T_Test Result.

One-Sample Test						
	Test Value = 0					
	t	Df	g. (2-iled)	Mean Difference	5% Confidence Interval of the Difference	
					Lower	Upper
Q1	.54	55	.00	1.643	1.3803	.9054
Q2	11.73	55	.00	1.429	1.1844	.6727
Q3	16.19	55	.00	1.286	1.1265	.4449
Q4	16.19	55	.00	1.286	1.1265	.4449
Q5	18.21	55	.00	1.321	1.1760	.4668
Q6	17.07	55	.00	1.268	1.1190	.4167
Q7	20.47	55	.00	1.179	1.0632	.2940
Q8	18.71	55	.00	1.179	1.0524	.3048

Table 3 shows that the first question of the questionnaire (I am concerned with the improvement features of security in cloud computing) is near to **Agree** category (Mean Difference = 1.643). Since this value is between lower, and upper range in *'Confidence Interval of the Difference'* so it could be considered as an acceptable value. However, the values of the questions respectively from 2 to 8 (Mean Difference = 1.429, 1.286,1.286, 1.321,1.268,1.179,1.179) are near to **Strongly Agree** and their values are between lower and upper range in *'Confidence Interval of the Difference'*. Accordingly, they could be considered as high accepted results.

The total results (Average of results) for all questions of the survey are as follows:

Average Mean=(∑mean)/N

Average Mean=(1.643+1.429+1.286+1.286+ 1.321+1.268+ 1.179+ 1.179) /8 =**1.3239**

Average Lower=(∑ Lower)/N

Average Lower=(1.3803+1.1844+1.1265+1.1265+1.1760+1.1190+ 1.0632 +1.0524)/8=**1.15354**

Average Upper=(∑ Upper)/N

Average Upper=(1.9054+1.6727+1.4449+1.4449+1.4668+ 1.4167 + 1.2940+ 1.3048 = **1.4938**

The analysis of total average results (As shown in Table 4) shows that the Average Mean Difference = 1.3239 is near to **Strongly Agree** category and this value is between Average lower, and Average upper range in *'Confidence Interval of the Difference'*. This result indicates a high acceptable value of the average of all questions.

Table 4 Average results

Average Mean Difference	95% Confidence Interval of the Difference	
	Average Lower	Average Upper
1.3239	1.15354	1.4938

9. Discussion and Conclusion

Cloud computing is suffering from various problems of confidentiality. Therefore, organizations or institutions need to double check the data in order to avoid problems of confidentiality that might happen to the cloud computing. Moreover, this will help to stay away from any problem that may damage any important data [22]. If problems of confidentiality happens in cloud computing, organizations might face many risks in the security issues.

The results of this research have presented the various levels of problems which impacted the security level of cloud computing in two phases. First, the organizations or institutions are very concerned in improving the security of cloud computing through the application of the authority model and dynamic classification of data model based on the multi-level security. Second, they prefer to develop the multi-key cipher algorithm in order to manage the encryption based on the level of security. Based on the results of this study, it is recommended that organizations must apply new policies in classifying the data into many security levels based on the nature of data to save time, and effort. Consequently, developing new encryption methods would be more convenient considering the nature of the security of data which reinforces safety in the implementation of the cloud computing in several organizations.

10. REFERENCE

[1] M. Boroujerdi and S. Nazem, "Cloud Computing: Changing Cogitation about Computing," World Academy of Science, Engineering and Technology, 2009.

[2] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Computer Communication Review, Volume 39 Issue 1, pages 50-55, January 2009.

[3] NIST, http://www.nist.gov/itl/cloud/index.cfm

[4] P. Mell and T. Grance, "The NIST Definition of Cloud Computing" Recommendation of NIST, Special

Publication 800-145, 2011.
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[5] http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[6] GTSI Group, "Cloud Computing – Building a Framework for Successful Transition," White Paper, GTSI Corporation, 2009.

[7] W. Jansen and T.Grance "Guidelines on Security and Privacy in Public Cloud Computing", NIST Draft Special Publication 800-144, 2011.
http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

[8] [T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Appications, 2010.

[9] http://www.idc.com.

[10] Ramgovind S, Eloff MM and Smith E. "The Management of Security in Cloud Computing" Information Security for South Africa (ISSA), Sandton, Johannesburg, 2-4 Aug, 2010.

[11] Z. Wang, "Security and Privacy Issues Within Cloud Computing" IEEE Int. Conference on computational and Finformation sciences, Chengdu, China, Oct. 2011.

[12] Dimitrios Zissis and Dimitrios Lekkas, "Addressing cloud computing security issues", Future Geberation Computer Systems 28, pp. 583-592, 2012.

[13] http://www.purplemath.com/modules/meanmode.htm

[14] http://www.investopedia.com/terms/s/standarddeviation.asp#axzz1ZyGlP8Xd

[15] http://www.investopedia.com/terms/v/variance.asp#axzz1ZyGlP8Xd

[16] Dimitrios Zissis and Dimitrios Lekkas, "Addressing cloud computing security issues", Future Geberation Computer Systems 28, pp. 583-592, 2012.

[17] Dave Abraham,"Why 2FA in the cloud", Network Security, Vol. 2009, Issue 9, Pages 4-5, September 2009.

[18] http://en.wikipedia.org/wiki/Two-factor_authentication

[19] Federal Information Processing Standards Publication 197,"Specification for the Advanced Encryption Standards (AES)", 2001.

[20] S. Fluhrer, I. Mantin, and A. Shamir, "Weakness in the Key schedualing algorithm of RC4", 8th Annual International Workshop on Selected Areas in Cryptography, Springer-Verlag London, UK, 2001.

[21] https://www.mathsisfun.com/definitions/range-statistics-.html

[22] Ahmed E. Youssef and Manal Alageel," A forA Framework for security Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012 ISSN (Online): 1694-0814

[23] R.K. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, B.S. Lee, TrustCloud: A framework for accountability and trust in cloud computing, in: 2011 IEEE World Congress on Services, SERVICES, July, 2011, pp. 584–588.

[24] Sabahi, F., "Cloud computing security threats and responses", IEEE 3rd International Conference on Communication Software and Networks (ICCSN), , 27-29 May 2011

[25] Carroll, M., van der Merwe, A. and Kotze, P., "Secure cloud computing: Benefits, risks and controls", Information Security South Africa (ISSA), 15-17 Aug. 2011

[26] Tanimoto, S. , Hiramoto, M., Iwashita, M., Sato, H. and Kanai, A., "Risk Management on the Security Problem in Cloud Computing" First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI), 2011

Mohanaad T Shakir is an Lecturer at Alburaimi University College, Oman. He .holds a B.S.C Degree in Computer Science from the University of Almamoon, Baghdad, Iraq; Post Diploma in Computer Security from University of Technology, Iraq and M.Sc. in Information Technology (MIT) from the University of Tenaga National(UNITEN), Putrajaya, Malaysia. He is a Ph.D. candidate in Information Communication Technology at the University of Tenaga National (UNITEN), Putrajaya, Malaysia. His research interests include Cipher Security, Computer-Aided Learning and Cloud Computing Security. He can be contacted at mohanaad@buc.edu.om.

DR. ASMIDAR BTE ABU BAKAR is an Senior lecturer from University Tenaga National, Malaysia. She received the B.S.C Degree in Computer Science from the Universiti Putra Malaysia and Master of Science (Computer Science) at the Universiti Putra Malaysia and completed her PhD at the Universiti Tenaga Nasional, Malaysi. Her research interest is Trust, Security and Privacy.

DR. YUNUS BIN YUSOFF is an Associate Professor at University Tenaga National, Malaysia. He completed B.Sc. in Computer Science and Master in Computer Application at the Pacific Lutheran University, and Ph.D in ICT at the Universiti Tenaga received the B.S.C Degree in Computer Science from the Universiti Putra Malaysia and Master of Science (Computer Science) at the Universiti Putra Malaysia and completed her PhD at the Universiti Tenaga Nasional, Malaysia. Her research interest is Trust, Security and Privacy.

DR. Ali Makki Sagher an Associate Professor at University of Alanbar, Computer college , Iraq. He completed B.Sc. in Computer Science , Master and Ph.D in Data Security, at University of Technology , Iraq . His research interests include Cipher Security, Information Security system and Cloud Computing Security. He can be contacted at ali_makki@uoanbar.edu.iq