CLOUD COMPUTING SECURITY CHALLENGES AND THREATS: A SYSTEMATIC MAP

Hassan Saad Alqahtani and Paul Sant
Department of Computer Science and Technology,
University Campus Milton Keynes (UCMK), Milton Keynes, U.K

ABSTRACT
Due to huge increment in consuming cloud computing services, there has been growing interest in improving the quality of the delivered services. The security aspect has been identified as one of the most critical customer concerns. In order to overcome the security issues and obstacles; there are a number of studies that have been done. In order to provide an efficient and effective solutions that are capable to overcome these obstacles; we need a better and comprehensive understating regarding these security issues This systematic review intends to identify the security challenges and issues. The outcome of the paper has enabled the creation of a systematic map that shows the current stage of knowledge about cloud computing security challenges. A major conclusion of this study is that there is a lack of empirical research and proposed approach, and there is a dire need for further investigation in order to overcome the expected challenges and benefits of the delivered cloud services.

KEYWORDS: *Cloud computing, cloud security, cloud security challenge, cloud security & systemic literature review.*

I. INTRODUCTION

Cloud computing has emerged as a new technology over the last decade and this implied new challenges. The National Institute of Standard and Technology (NIST) defines the cloud computing as "*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*" [1]. The demands on cloud computing services are increasing continually; the cloud computing market was worth $37.8 billion in 2010, and it is expected to reach $121 billion in 2015 [2]. Besides that, there is a huge interest in consuming cloud services through smart devices; and the consumer and enterprise market for cloud services provision through mobile applications is expected to rise to $46.90 billion by 2019 [3]. The reason that drives to this continuous growth and increased demand on the cloud computing services can be summarised into the following:

- The core features of cloud computing technology: pooling resources, elasticity, on-demand, pay-per-use and ubiquitous access [4].
- The diversity in the deployment methods (public, community, private, hybrid).
- The diversity in delivery methods (Infrastructure as a Service, Platform as a Service, Software as a Service) [5].

Similar to other technologies the cloud computing have some open issues and limitations. The security factor is one of the most critical concerns and roadblock that prevent moving to the cloud. According to [6], security is one of the four main concerns of the majority of cloud customers. There are some studies that concern about the cloud computing from the security perspective. For instance, [7] argue that the cloud computing security drawbacks could be summarised into ten points, five out of ten points are related to the security aspect: availability, data lock-in, confidentiality, auditability, and malware/bugs inside the system. There are two core weaknesses with [7]; the first defect is lacking of details that might help to enhance understanding the identified obstacles; for instance, the

authors address the auditability as an issue; but there is a critical lack in 1) essential information that explains why the audibility is an issue, and 2) real cases as examples. The second defect is the study date; there are some issues have been solved, there are other have been considered as a law and regulations issues, and there are new issues have not addressed yet. Additionally, there is a survey; that has been published by [8], attempt to show a number of vulnerabilities, threats, and attacks that associated with cloud computing security. The study assigns the identified vulnerabilities, threats, and attacks with the proper solutions. However, the new cloud computing models; for instance, multi-clouds, mobile-cloud, and ad-hoc cloud have not included via this study.

However, there is no such systematic review study that is 1) up-to-date, 2) comprehensive and accurate. Duo to that, this study will look into the existing literature of cloud computing security; and that will be implemented via searching, filtering, classifying, and analysing the previous related studies; which will provide detailed and comprehensive overview about what is already known regarding cloud computing technology in term of security. Additionally, it will identify the potential challenges and threats of developing, providing, managing, and consuming the cloud computing services.

The paper's structure could be explained as follows: Section II summarises the applied review strategy and explains the followed review process. Section III discusses the review outcomes. Finally, Section IV will sum up the study outcomes.

II. REVIEW METHOD AND CONDUCT

2.1 Review Strategy

The Kitchenham systematic review guideline [9] [10] has been used in order to define a clear strategy for implementing this systemic review. The mentioned guidelines steps could be summarised as follows:

- Defining the study's questions and scope.
- Defining the research's strategy and the data sources.
- Collecting the related papers.
- Applying quality assessment test.
- Extracting and analysing the papers' contents.
- Answering the review's questions.

2.2 Review Research Questions

As we mentioned before, that this review has been developed in order to support and prove the study assumption; which is 'the single cloud storage cannot be used as a secure and trust method for protecting sensitive data'. For that, there are two research questions have been identified.

- ***What is known about the cloud computing security?***

This question aims to provide a general overview about what is known about the security aspects of the cloud storage. Through the review process there is a number of papers focus on security of cloud services from different perspectives; these perspectives can be shown in Table 1.

Table 1. Cloud Security perspectives

Perspective	The Involved Responsibilities
Owner	Resource Physical Protection – Recovery – Management – Auditing – Privacy – Network – Virtualisation – Policies
Developer	Software – Authentication – Management – Monitoring – Privacy – Integrity
End user	Password – ID – Access Platform – Social Engineering - Phishing

- ***What are the main security challenges and issues of cloud computing?***

This question aims to address the objective of this review, which is highlighting the challenges and issues of cloud computing in terms of security and data protection. Besides that, this review will identify which aspect has the most critical weaknesses. In order to that, the addressed challenges and issues have been collected, extracted, analysed, and documented in the results part.

2.3 Keywords and Data Sources

The search process has been implemented over four digital libraries (ACM digital Library, IEEE Xplore, Science Direct, and Springer Link); these libraries contain the most reliable, diverse, and well-known publications that related with the cloud computing field. The searching language has been specified to "English", and the publications' data has been limited to 2010 to February – 2015. Table 2 shows the searched keywords.

Table 2. The researched keywords

Category	Keywords
Cloud Computing Technology	Cloud, cloud computing, cloud security, cloud challenge, cloud issues, cloud threat, cloud attack, cloud vulnerability, cloud vulnerabilities, cloud privacy, cloud protection, cloud data integrity, cloud data safety,
Cloud Computing Related Technologies	Cloud trust, cloud virtualisation security, cloud authentication, authorisation , cloud ID management, cloud encryption, cloud DoS, DoS, DDoS, cloud VM, cloud image, secure API,

2.4 Selection Procedure

As a part of the studies selection procedures, the selected studies had to go through four phases. In order to select the most relevant studies and enhance the quality of the extracted data; these phases and the number of publication of each phase can be shown in Table 3.

Table 3. The researched keywords

Phase		Number of Selected Publications
1	Search by keywords, and select the related publication based on the title.	932
2	Read the abstract, and scan the publications to decide if it is related or not.	613
3	Read the contents.	329
4	Apply the quality assessment.	137

The 1st phase bases on the used keywords; and the selection has been occurred based on the publication's title. The 2nd phase was focusing on the publications' abstract, which had been selected at the 1st phase. In some cases, there is a kind of lacking abstract; where the abstract cannot provide the paper concept clearly; for that, the sub-titles, figures, tables, and main contents will be scanned in a brief way.

Worth to mention, that after the 1st phase there is a pilot test has been carried on a random publications (25), in order to clarify the expected data and information types that will be execrated through this review. The 3rd phase was reading the selected publications, and identifying some important information; for instance, the study's type, study's scope, and the study's aim. Finally, the quality assessment has been applied in order to identify the final selected publications. The applied quality assessment consists of nine factors, which can be shown in Table 4. After applying the quality assessment, all the publications that have a score less than 5 will be discarded, in order to enhance the quality of the carried review.

Table 4. Publication Assessment Criteria

Criteria	Question
Research Aim	*Does the publication identify the research aim/s clearly?*
Research Design	*Does the publication explain the applied research methodologies?*
Contribution	*Does the publication outline the added value and the contribution?*
Data Collection	*Does the publication explain the applied data collection methodologies?*
Sample	*Does the publication provide information about the sample (type, size…etc.)?*
Data Analysing	*Does the publication provide a clear explanation regarding data analysing process?*
Research Outcomes	*Does the publication state the research outcomes clearly and discuss these*

	outcomes?
Cloud Computing	*Is the publication related with the cloud computing?*
Cloud Computing Security	*Is the publication related with the cloud computing security?*

III. RESULTS AND DISCUSSIONS

3.1 Systemic Review Results

In order to provide a comprehensive and complete answer for the ***RQ1***, there is information has been extracted; that information was used to render a statistical overview regarding what is known about the cloud computing security. Figure 1 represents the selected publications based on the searched databases, and the publishing years. The number of publications varies between 16 publications in 2010 and 37 at 2013. The IEEE has the majority of publications by 52; and the Springer got the lowest number of selected publication which is 20.

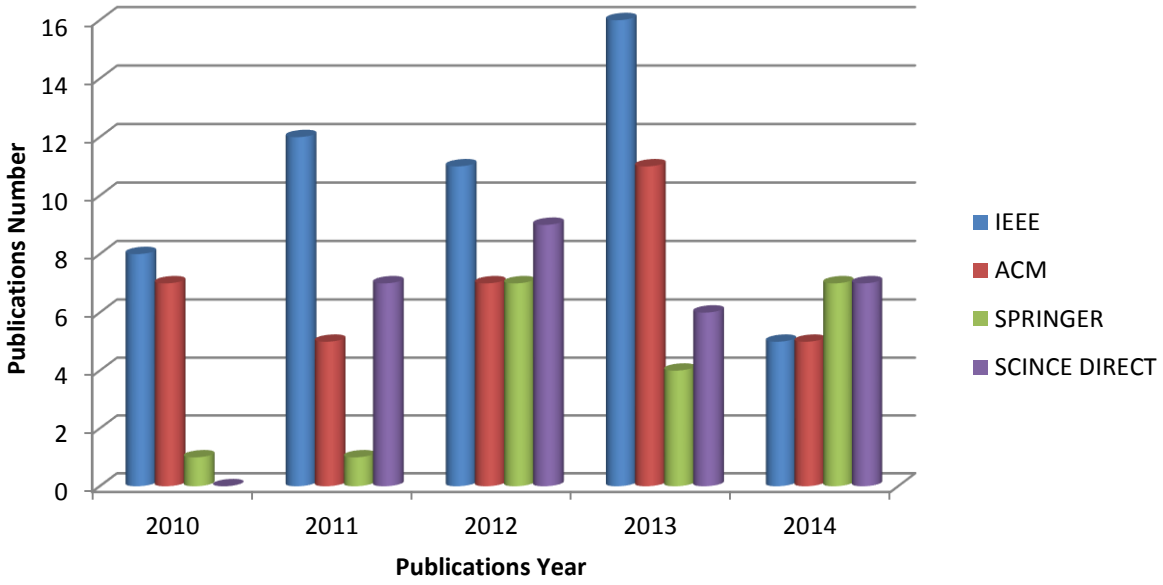

Figure 1. The Publications' Number Based on the Year and the Database

Figure 2 illustrates the number of published studies for each year. The publications numbers in 2012 and 2013 increased to reach more than 60 publications for both years; which represents the rapid increment of interesting at that technology, and that practically driven by the continues and developed cloud computing industry.

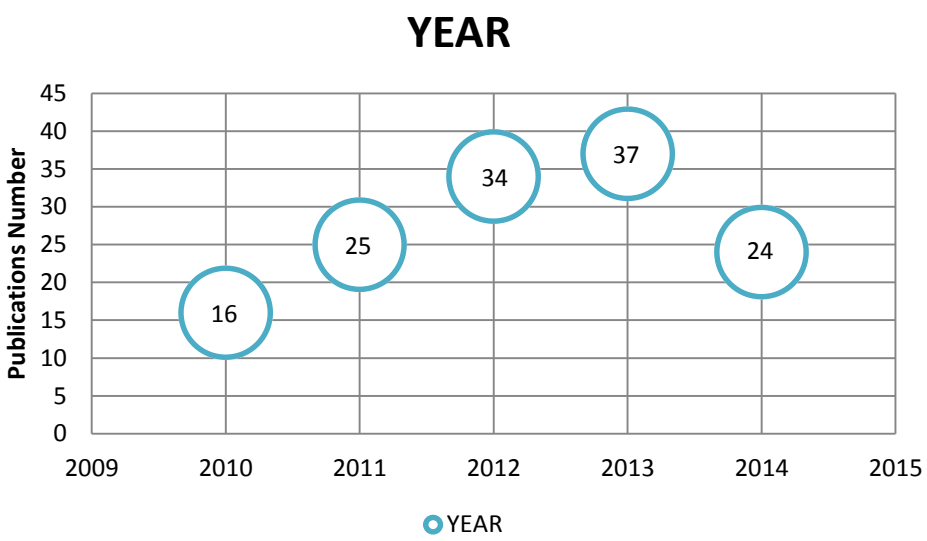

Figure 2. The Publications' Number for Each Year

Out of the selected publications, the Springer has 20 publications; which represent about 15 % of the selected publications, and it is the least data source. However, IEEE has about 38 % of the involved publications, and that percentage make IEEE has the largest number of selected publications, and that can be shown in Figure 3, which represents the share of each database.

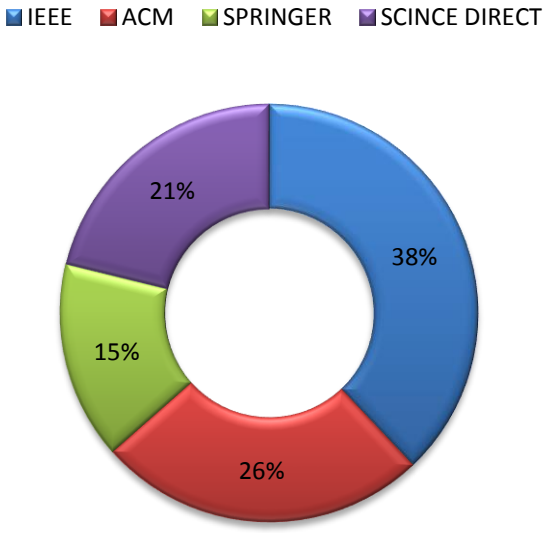

Figure 3. The Selected Publications Based on Database

The selected publications have been classified into specific classes based on their concentrate and aim. The classes are: case study, evaluation and comparison, analysis, proposing framework, and challenges; and that classification can be shown in Figure 4. Apparently, the majority of selected publications aim to highlight the challenges/issues, and there is only about 14% out of the selected publications proposed solutions. That variation shows clearly the gap between the existing issues and the proposed solutions.

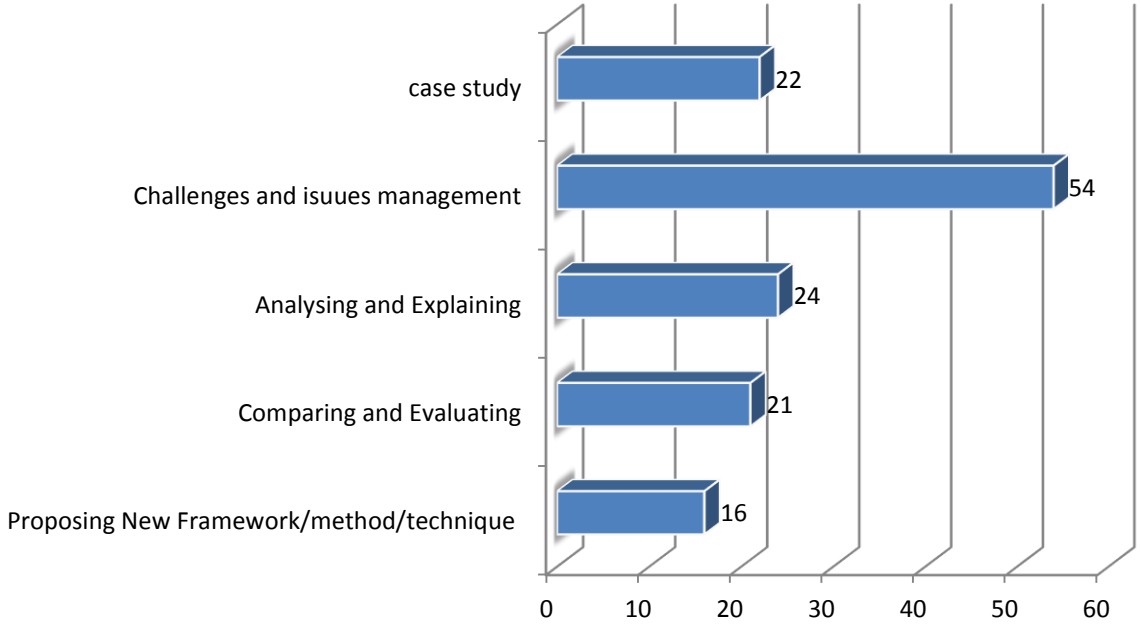

Figure 4. The Selected Publications based on the contents

In addition, there are about 47% of the selected publications are focusing on the cloud computing security, while there are less than 25% that is concentrating about relative technologies; for instance, encryption techniques, authentication methods, and communication protocols; and Figure 5 illustrates the publications based on the scope.

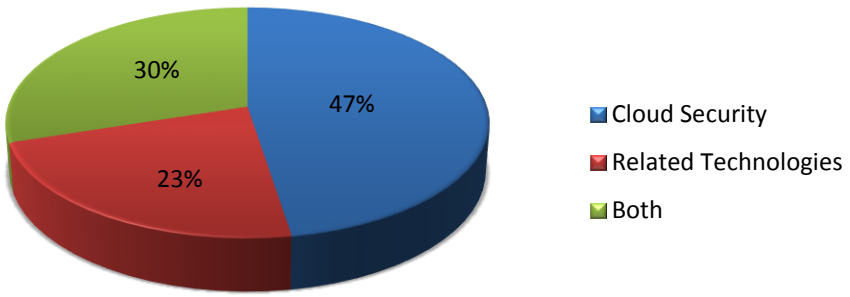

Figure 5. The Selected Publications based on the targeted aspects

Figure 6, categories the selected publications according to the applied research methodologies. Obviously, the majority of publications use surveys and systemic studies as research methodology; and that shows clearly the lack of empirical studies.

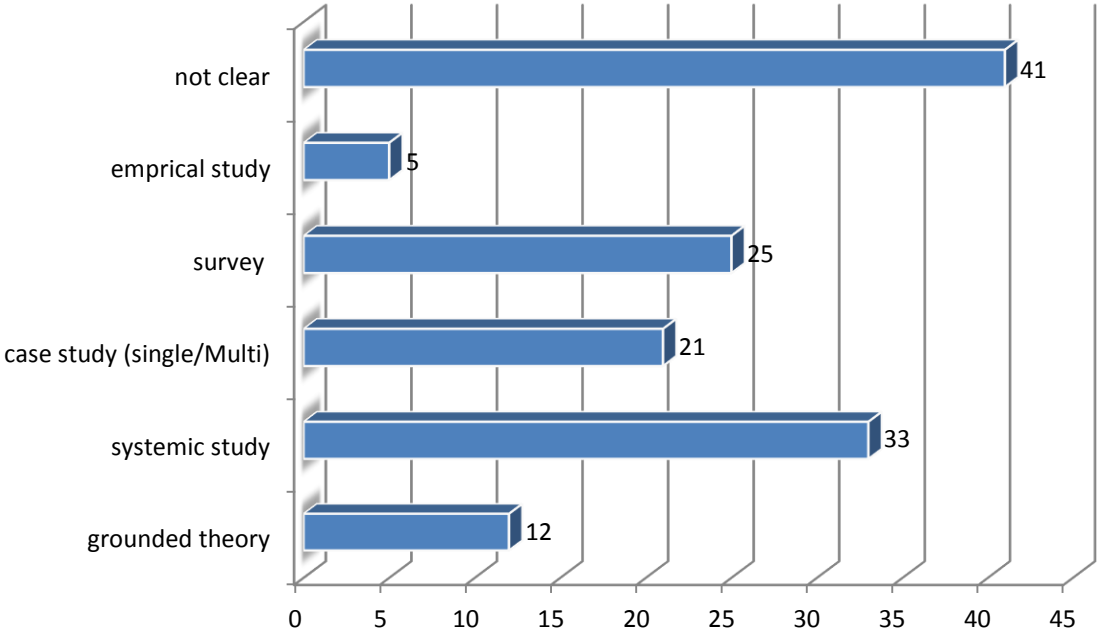

Figure 6. The Selected Publications based on the applied research methodology

3.2 Cloud computing security challenges and issues

In order to answers the RQ2, there selected publications have been analysed due to identify the cloud computing security challenge and threats. The extracted challenges and threats have been classified into six categories. This classification bases on the level of the challenges/threats; these level are: trust, access, internet, software, computation, and virtualisation. Figure 7 summarises and outlines this classification and the identified challenges and threats. These categories are closely related, and each one having an impact on the others. For instance, the lack of good practice while developing the service frontend may increase the possibility of un-authorised access. These challenges have to be studied together as one set of challenges. The majority of the identified challenges are associated with computation and access level (51%). For the computation issues, the identified challenges are: sanitisation, malware, cryptography, and storage. According to Wang *et al.* storage security is a key factor that impacts on the delivered service's QoS [11]. In fact, the concept of outsourcing data storage can raise a lot of concerns from the customer's perspective; the customers would like to know where and how their data will be stored and who will have access to it. All these concerns can be associated with the third party as well. On the other hand, the authentication, and the physical access associated with the access level. The authentication security issues vary between the authentication methods, authentication attacks, and ID management. Usually, the cloud service providers combine the user ID and password to authenticate the user's identity, but they vary in the password techniques. The most common technique is a simple text password, which, according to Hart cannot provide the required level of authentication [12]. However, that does not mean that the other issues are not critical. In addition, any developed approach should consider the other challenges, otherwise that might led to expose the system.

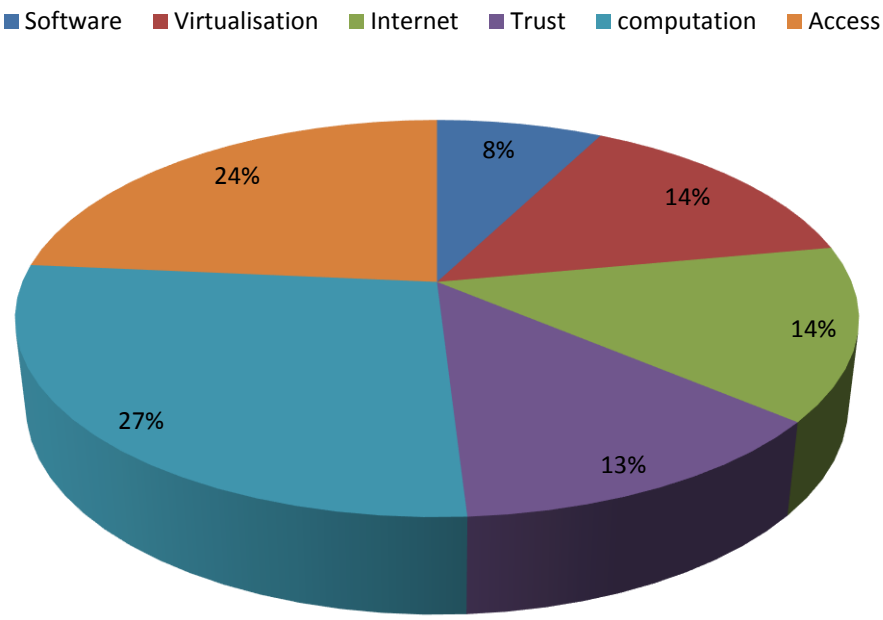

Figure 6. Cloud computing security issues categories

IV. CONCLUSIONS AND FUTURE WORK

To sum up, this systemic literature review demonstrates the nature of the current literature regarding the cloud computing security challenges/ issues. This review finds that more than 88% of the investigate studies in this area are not proposing any framework or techniques as a solution for the addressed security issue/challenge. In addition, it illustrates that less than 4% of the covered studies are empirical studies, and about 30% have no clear methodology. On the other hand, there is critical need about developing critical studies that able to provide better understanding for the security challenges and threats. Therefore, there is a need for studies that propose solution/approach, which describe the challenges and detail the developed solution/approach.

It is obvious that Future work will involve further investigation to examine these challenges and provide a better understanding of the existing cloud computing security challenges. The further investigation will help to develop approaches/frameworks that capable to solve these challenges and overcome the identified obstacles. Also, the access, computation, and storage aspects will receive specific intention in order understand the reasons behind the inefficiency of existing solutions, and develop a new framework to overcome existing obstacles.

REFERENCES

[1] Mell, P. & Grance, T. 2011, "The NIST definition of cloud computing".
[2] MarketsandMarkets, 2010. Cloud Computing Market: Global Forecast (2010 – 2015). Market Research Company and Consulting Firm, Available at: http://goo.gl/02tRN [Last Accessed on July, 2014].
[3] MarketsandMarkets, 2014. Mobile Cloud Market by Application (Gaming, Entertainment, Utilities, Education, Productivity, Business & Finance, Social Networking, Healthcare, Travel & Navigation), & By User (Enterprise User, Consumer) - Worldwide Market Forecast and Analysis (2014 - 2019). Market Research Company and Consulting Firm, Available at: http://goo.gl/MJdIFC [Last Accessed on July, 2014].
[4] Josyula, V., Orr, M. & Page, G. 2011, *Cloud computing: Automating the virtualized data center*, Cisco Press.
[5] Furht, B. & Escalante, A. 2010, *Handbook of cloud computing*, Springer.
[6] Bouayad, A., Blilat, A., El Houda Mejhed, N. & El Ghazi, M. 2012, "Cloud computing: Security challenges", *Information Science and Technology (CIST), 2012 Colloquium in*, pp. 26.
[7] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A. & Stoica, I. 2010, "A view of cloud computing", *Communications of the ACM*, vol. 53, no. 4, pp. 50-58.

[8] Modi, C., Patel, D., Borisaniya, B., Patel, A. & Rajarajan, M. 2013, "A survey on security issues and solutions at different layers of Cloud computing", *The Journal of Supercomputing*, vol. 63, no. 2, pp. 561-592.
[9] Kitchenham, B. 2004, "Procedures for performing systematic reviews", Keele, UK, Keele University, vol. 33, no. 2004, pp. 1-26.
[10] Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J. & Linkman, S. 2009, "Systematic literature reviews in software engineering – A systematic literature review", Information and Software Technology, vol. 51, no. 1, pp. 7-15.
[11] Wang, C., Ren, K., Lou, W. & Li, J. 2010, "Toward publicly auditable secure cloud data storage services", *Network, IEEE*, vol. 24, no. 4, pp. 19-24.
[12] Takabi, H., Joshi, J.B.D. & Gail-Joon Ahn 2010, "Security and Privacy Challenges in Cloud Computing Environments", *Security & Privacy, IEEE*, vol. 8, no. 6, pp. 24-31.

AUTHORS

Paul Sant joined the department of Computer Science and Technology (UoB) in September 2005 as a lecturer and he became a Senior Lecturer in September 2006. He was promoted to Principal Lecturer in August 2011. Dr. Paul completed his PhD from King's College, London in 2003 with a thesis entitled "Algorithmics of edge-colouring pairs of 3-regular trees" and prior to this, a BSc. in Computer Science from the University of Liverpool (1999). He is an active member of the British Computer Society and a Chartered Information Technology Professional (CITP) as well as being a fellow of the Higher Education Academy. In January 2013 Paul was appointed to a seconded position of Associate Dean, UCMK.

Hassan Alqahtani started his PhD March-2014 at university of Bedfordshire. His research interest includes cloud computing, mobile cloud computing, cyber security, and encryption. He received his Master degree from Teesside University in 2012, and his Postgraduate certificate from Essex University in the Telecommunication and Information System.