An Investigation of the Most Critical Security Vulnerabilities in Cloud Computing in Saudi Arabia

Amani M. Ghazzawi, Fatimah M. Alqahtani, and Fahd S. Alotaibi
Faculty of Computing and Information Technology, King Abdulaziz University,
Jeddah, Saudi Arabia
Email: Amani.ghazzawi@yahoo.com, fatimahalaboud@hotmail.com, fsalotaibi@kau.edu.sa

Sjaak Laan
Principal IT Architect, CGI
Email: sjaak.laan@gmail.com

***Abstract*— Cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources can be rapidly provisioned and released with minimal management effort or service provider interaction"[1]. While cloud computing has several benefits, some organizations do not use it because of security concerns. This study was conducted to explore threats, vulnerabilities, and security risks in cloud computing, and present some solutions to those concerns. This paper has three main objectives. First, identifying the reality of cloud computing security generally. Second, covering the most critical security vulnerabilities, threats, and issues in cloud computing as well as suggestions to mitigate them. Third, clarifying security countermeasures used in Saudi Arabia in medical, commercial, and academic fields, and commercial fields. Logical and administrative data security, service level agreements, data leakage, customer monitoring, and the existence of loopholes are the major security issues in the cloud computing. Using private cloud, multiple frames of data storage, improving content security, data integrity, and service level agreement, encryption mechanisms, and access control services are some solutions to mitigate cloud computing security concerns.**

I. Introduction

A. Background and Motivation

The world is witnessing a remarkable transformation through the adoption of innovative technical solutions and the transition to social networks. Cloud computing represents a significant growth in the field of technology; it is considered the way to the future of informatics. Using cloud computing has become one of the main pillars of the progress of nation and growth. The concept of cloud computing not limited in the private sector, but extends to government sectors as the government cloud. It aims to move all data and computing resources of ministries and government agencies to the cloud. Technical infrastructure must be developed to support all services, such as healthcare, education, transportation and commercial banks. However, the researchers see that Saudi Arabia received the idea of cloud computing with some fear and lack of acceptance from the most private and government sectors, mostly because of information security and privacy concerns. As an example, according to Bronk and Tikk-Ringas [2], Saudi Oil Company "Aramco" was exposed to an aggressive electronic attack in mid-2012, in addition to numerous previous attacks. More recently, Wass [3] reported on November 19, 2016, that the electronic security center monitored cyber-attacks from foreign third parties, targeting services from government agencies in Saudi Arabia. Using the disruption of servers and devices, the attacker planted malicious software to disable user data. The evolution of digital violence and the impact of cyber-attacks should direct public and private sectors to work more efficiently on the protection of information security, especially now these cyber-attacks not only affect companies, but the entire Saudi people. Consequently, the Security Center recommended to take necessary measures to protect electronic systems, reducing remote access through the VPN virtual network, and service access to the Remote Desktop RDP. This paper presents a reflection of the security practices used in cloud computing. Also, the researchers pointed out cloud computing vulnerabilities, threats, current and future security risk. as well as solutions to these issues. The researchers conducted a survey on some of the health, academic and commercial sectors in Saudi Arabia to detect the state of cloud computing security in Saudi Arabia.

B. Current Situation of the Target Country

Research conducted by the Communications and Information Technology Commission recently [4] showed that the cloud computing services market in Saudi Arabia achieves an increasing growth. In 2014, 189 million Saudi riyals was spent on cloud computing services. A significant growth occurred over the past

Manuscript received December 21, 2016; revised April 1, 2017.

doi: 10.12720/jait.8.3.165-171

years, where spending increased by 373%. Cloud computing services is expected to grow to over 4.1 billion Saudi Riyals by 2019.

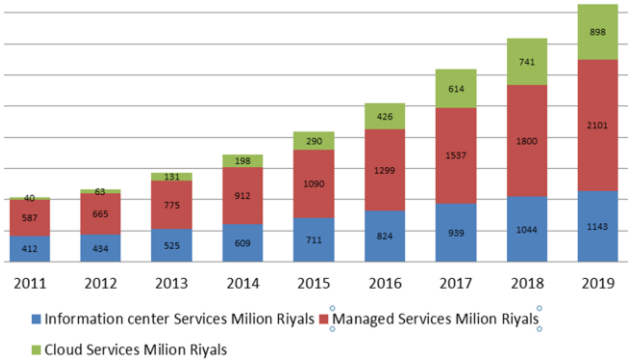

Figure 1.Growth rate of market information centers, managed services and cloud computing services during the past and future years in S.A

The Communications and Information Technology Commission conducted a detailed study on the public and private sectors to assess the current situation in the use of cloud computing [4]. The study included the prevalence and use of cloud computing and the factors motivating and impeding her. The study results indicated that most sectors in Saudi Arabia prefer direct control of internal processes, using their own datacenters. Also, most of the sectors are free to put their servers in commercial information centers, or host their systems by the share model on the site (as participation in ICT service providers to manage the infrastructure of their servers), because of security concerns.

Using cloud computing, private sectors lose control over the part of their operational processes, and this loss of control is linked to information security concerns. This poses a challenge to the market in developed and emerging countries, and rises fear in the relatively less mature countries, including Saudi Arabia. In addition, cultural factors play a role in increasing the effect of inhibiting factors, where enterprises in the Kingdom take great care of information security and are very related to risk it, so they prefer to maintain their control and manage as many of their activities internally, CITC [4]. While sectors in Saudi Arabia are getting more familiar with IT security standards, security concerns remain a key element in mass adoption of cloud computing in many organizations. After recent electronic attacks in many countries, including Saudi Arabia, information security has become a serious challenge to the long-term business, CITC [5].

A study conducted in Saudi Arabia by EMC [6] revealed that 44% of public sector companies in Saudi Arabia had already applied or are planning to use a cloud computing model. However, 48% of the companies expressed their concerns about privacy and security conditions associated with public cloud models [6]. Therefore, security problems in cloud computing are considered weaknesses that must be addressed.

C. Research Problem

With rapid advances in information technology, institutions, companies, and individuals put more information in the cloud. At the same time, uncertainties began to grow about the availability of a safe environment, and therefore, most of the sectors are reluctant to put their data in the cloud. Cloud computing security, privacy, and data protection concerns reduced the growth of cloud computing. This study aims to finding a solution for cloud computing's many security risks.

D. Key Contributions

This research is gaining importance, as the rapid growth in cloud computing has significantly increased security concerns in private and government agencies. Insecurity is a major obstacle to wide spread adoption of cloud computing. Increasing prosperity has led to increasing cloud computing security challenges for consumers and service providers. The importance of research is in enabling researchers and specialists in the field of security in understanding cloud related risk and helps them finding workable solutions to mitigate risk. The main contributions of this study are:

1) Identify the environment of cloud computing security in Saudi Arabia.
2) Register threats, vulnerabilities, and risk related to cloud computing.
3) Propose recommendations to resolve those problems.
4) Investigate security countermeasures used in Saudi Arabia and possibile of investments in datacenters.

E. Research Methodology

This study is based on a descriptive and analytical approach by using the systematic review, through addressing the weaknesses and the most important security issues and identify threats in cloud computing in medical, commercial, and academic sectors. The research also provides a description of some of the solutions and how they can cope with these risks in the future. Systematic reviews are undertaken to summarize the actual substantiation in various sectors of Saudi, identifying the gaps in present research and providing a scope for new research activities. The researchers gathered information from a range of documented studies and academic sources that deal with cloud computing challenges and security issues. A questionnaire was used, which included three main questions and sub-questions about the security of cloud computing in academic, medical, and commercial sectors in Saudi Arabia.

II. Data Collection

A. Target Audience

We have conducted the questionnaire in three sectors in Saudi Arabia (academic, medical, and commercial), addressing security issues and challenges faced while applying cloud computing in the organizations. We found that finding security experts in cloud computing in various sectors in Saudi Arabia, willing to respond to our

questionnaire was difficult. Nowadays, health centers are looking for smart solutions to manage their business, and electronic systems have become an important part of the solution. Aljabr [7] demonstrates that health centers rely on cloud computing to enhance productivity and restructure information systems. However, challenges remain related to the security measures, to protect files from attacks and privacy breaches. For example, the intensive care unit should provide the highest degree of safety and must identify the persons having the authority to access to patient data.

B. Questionnaire Design

The questionnaire comprises three main questions and a number of sub-questions; each of which is an open question. We decided to use open questions aiming to have variance in the answers. The questionnaire was directed to engineers and experts in cloud computing, as we expect them to have sufficient information. The type of questions enables us to understand how cloud computing is applied in Saudi Arabia, as well as expand our information in this field. We targeted three sectors in Saudi Arabia: academic, commercial, and medical. Some organizations replied to us that they can't answer the questionnaire's open questions because they need much time. However, we got good information that helps us to complete our research.

TABLE I. QUESTIONNAIRE DESIGN

	Questions
Q1:	What is the reality of cloud computing security?
	A: What are the current security technologies are used to face the challenges of cloud computing?
	B; What are the security policies for the public and private cloud?
Q2:	What are the various security techniques are used by cloud computing providers to prevent attacks?
	A: How can your organization protect customer's data from attacks in the cloud?
	B: How can the Cloud service provider control access to data integrity for the client in the clouds?
	C: What are the appropriate encryption technologies that you use to protect data?
Q3:	How can you deal with the expected cloud computing security problems in the future?
	A: What are the proposed recommendations for dealing with future security problems?

III. RESULTS AND DISCUSSION

When analyzing the answers to the questionnaire, we noticed that some sectors in the country are reluctant to use cloud computing. Military Hospital reported that they concluded cloud computing is easy to attack, and the risk to data leakage is significant. These information security and privacy concerns in the cloud is one of the reasons the hospital does not use cloud computing. King Abdullah Medical City believes that cloud computing security is a critical consideration, since we are living in the era of innovation of technology. Cloud computing requires new methods to secure remote information, while providing secure access for the owner of the data. Hackers' attacks, service denial attacks, and leaking personal information are some of the stated security concerns related to the cloud. Implementing encryption, keeping software and operating systems up to date, setting strict permission for users on servers, and scanning hackable ports are some recommendations which would mitigate the stated risks.

In the Commercial sector, Alnafitha International Information Technology responded by listing some of the weaknesses in their cloud model. They also mentioned some of the techniques used to mitigate these weaknesses. The company illustrated their point of view: using a private cloud model helps ensure data protection, as information is stored behind a firewall. Gulf systems and packaging company believe it is crucial to protect data from attack. As a result, they do not use cloud computing now and they do not plan to use it in the future because of the security issues. The company has limited the use of cloud services only to Email services.

In the academic sector, the questionnaire revealed the University of Taibah uses cloud computing, backed up by using private servers. They feel this hybrid model is the most important technique to save data. Taibah University pointed out that cloud computing has facilitated a lot of things, like maintenance and faster access to data in case of hardware or software failures. Taif University does not use cloud computing because of cost and security concerns. However, they use Microsoft cloud based Email services to students. They said that it is better to be independent and having the right to control their own. This is the case of most of the universities in Saudi Arabia. King Abdullah University (KAUST) demonstrates that as KAUST embarked on the journey of cloud migration, security was at the heart of this mission. The KAUST Information Security Office is accountable and responsible for protecting all information assets around the university. With the cloud, they started sharing some of the information security risks with the cloud service provider but it cannot let go of the accountability they have. KAUST's responsibility for protecting assets depended on the cloud service model that houses their information. KAUST engaged into all three service models with their cloud service provider (SaaS for email and document collaboration services, PaaS for all our business applications running on top of SAP, and IaaS for all others). The security responsibility shifts from the service provider to KAUST as you go down this list from SaaS to IaaS. Table 1 shows the cloud computing security issues and suggestions that we have obtained through the survey.

IV. LITERATURE REVIEW

Three primary models are classified as cloud computing services: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Krishna et al. [8] considered security issues in all three cloud computing models. Threats and vulnerabilities in the OpenStack cloud management software are discussed by Hatwar and Chavan [9], and they demonstrate countermeasures for each risk/vulnerability. Dahbur et al. [10] give valuable

suggestions to mitigate cloud computing risks. Understanding the concept of cloud computing and its abilities is necessary to detect risks, threats, and vulnerabilities related to the cloud computing. Preforming security evaluations, understanding security rules, and enough experience are essential elements when choosing a suitable cloud provider. Organizations should be careful in selecting a cloud service provider; it should be based on an explicit contract between the business objectives and IT.

Alshammari and Bach [11] shed light on some of the crimes and security issues. They present a vision for a service level agreement in cloud computing, that is includes control over the data management policy, determining the location of the data, the duration of unavailability of the data, and trust between the client and the service providers. Derfouf et al. [12] in their study provide a broad concept of various threats, vulnerabilities, and challenges in cloud computing to discover new gaps and to find appropriate solutions in the future. The increasing use of cloud computing enables hackers to find loopholes to see users' data. Also, they propose a solution to the problem of secure data storage in the cloud environment using encryption mechanisms of the OpenStack system that offers high protection, to make it impossible to read the data in the case of a privacy breach. Perez-Botero et al. [13] describe hypervisor security vulnerabilities to real attacks. They were the first to suggest and integrate three hypervisor vulnerability classifications: by hypervisor functionality, trigger source, and attack target. The integration of the three classifications clarifies the different hypervisor modules and runtime spaces during a successful attack. Perez-Botero et al. [13] believe their study can assist in better establishing users' security needs and determining the scope of the solutions that might be proposed to address them.

Now that we have a good overview of risks, threats, and vulnerabilities in cloud computing, we would like to view some suggestions to relieve those concerns. Masky et al. [14] propose the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach, which is used to obtain successful results by identifying risks of cloud computing. The OCTAVE approach is different from other cloud computing evaluation methods because it concentrates on information evaluation. Information security scheme is not present in cloud computing which makes risk identification not perfect (it is the issue of the risk identification).

TABLE II. THE QUESTIONNAIRE RESULTS

Sector	Organization name	Current situation	Security issues and challenges	Solutions and suggestions
Medical	Military Hospital	They do not use cloud computing because of security and cost reasons.	NA	NA
Medical	King Abdullah Medical City	Their organization is using very basic protections methods. It is not 100% secure, but it makes it difficult for attackers to gain full access. For example, they keep their systems and software up to date.	There are many technologies used to secure cloud computing. However, it's hard to apply some of them either for being expensive or inefficient. I believe the biggest challenge is the lack of tech savvy who could operate these technologies. Also, they believe that information security is very untapped subject in Saudi Arabia and that is dangerous.	Cloud service provider can control access to data integrity for the client in the clouds by encrypting the data and make the client be the only one who has the (private key) to decrypt the data. But that might raise other concerns. The appropriate encryption technologies that they use to protect data are RSA on the website; they use SSL to make sure the connection between the client and the website is secure. There are some security techniques used to prevent DDOS attacks. Another technique is to use sandboxes (also known as honey pots) to prevent hackers from obtaining access to the actual network and systems. The proposed recommendations for dealing with future security problems are: • Keep your system up to date. Create daily backups. • Secure your system from the public exploits. • Secure ports. • Provide limited access to the employees that is less than root or administrator. • Hiring experts and learn technology trends. • Keep learning and updated.
Commercial	Al-Nafitha International Information Technology	With the development of the technology market, the experts are worried about increased security needs for cloud computing. Security issues in cloud computing are one of the major concerns that the company is facing.	Challenges: • Trust and law agreement between provider and customer • Multitenancy and multi-instance architecture • Identity and access	• Use private clouds • Create stronger passwords • Secure your data transfer channels • Know your software interfaces • Encrypt the data

			management • More data in transit issues • Security in the cloud • Cloud compatibility issues • Compliance of the cloud • Standard design of cloud technology • Monitoring while on the cloud	
Commercial	Gulf Systems Packaging Company	The company uses two servers for data storage, and firewalls to secure them. One server is allocated to save a backup in the event of a breakdown. Currently, the company does not use cloud computing because of privacy and information security.	NA	The company does not use cloud computing and does not look to use it in the future because of the security issues.
Academic	King Khalid University	They do not use cloud computing because of security and cost reasons.	NA	NA
Academic	King Abdullah University	As KAUST embarked on the journey of cloud migration, security was at the heart of this mission. The KAUST Information Security Office is accountable and responsible for protecting all information assets around the university. With the Cloud, we started sharing some of the information security risks with the Cloud Service Provider but cannot let go of the accountability we have. Our responsibility for protecting assets depended on the cloud service model that houses our information. KAUST engaged into all three service models with our Cloud Service Provider. These are: 1. SaaS for email and document collaboration services 2. PaaS for all our business applications running on top of SAP 3. IaaS for all others	• Responsibility of monitoring and SLAs around incident response. • Another major challenge is the vendor lock-in. If KAUST decides to change the current cloud service provider in the future, it will have to venture into a lengthy and complex migration project similar to the one we had during migration from our on-premise systems to the cloud service provider.	Encryption is employed for data at rest and data in motion in all models. TLS is used for securing data on the move with at least AES 128-bit encryption. Storage based encryption is used for data at rest and options available vary from 56 bit all the way up to 256-bit encryption based on the classification of the data and its sensitivity.
Academic	Taif University	Focuses on the use of the data center, but they do not use cloud computing for reasons of security and cost.	Not to use cloud computing in Taif University is due to two points: First, it was the objection of the security risks. As the Taif University was keen on their data and they worried about the security and privacy, the university administration decided to use only the internal hosting. Second: Infrastructure availability – the university does not use an external host, as they do not want to be tied to a third party. In addition, in case of a malfunction, they do not want to call parties outside the university, as this increases costs.	Taif University, said it is seeking a future in the next two years to move towards making some applications hosted externally. But so far, there is opposition from the physical point of view, has been the project view of Mobily and King Abdulaziz City the same ideas, however, the university did not go to this thread so far.
Academic	Taibah University	Uses cloud computing, backed up by using private servers.	Data leakage	• Back up by using private servers • The trend towards the use of participatory cloud computing applications in the promotion of technical performance.

Ismail et al. [15] have pointed to security problems of the cloud: the logical data security, administrative security, which would reduce the trust between the customer and the service providers, which included inadvertent access, and other problems. They suggested some security measures which based on few courses such as cryptography. Moreover, representing a methodology that allows anyone to create phase cloud safe system. They also pointed out using the framework of a multi-specialists in engineering to enable security for data storage in the cloud. Doinea and Pocatilu [16] present a study on content security in cloud security applications that is necessary for research and technological development of cloud computing areas. Doinea and Pocatilu [16] propose a security approach to improve content security during the classification of vulnerabilities in different levels and good integration of security controls. They also point out the security measures that the Ministry of Information Technology should take, including the security of networks. They also show a cloud based on library information system as well as some adjoining mechanisms that are used together to have digital data and metadata. This will serve the libraries and infrastructure development to provide digital content.

In the technical field, Jensen et al. [17] illustrate some technical cloud computing security issues. First, they show the relevant technologies involved in cloud computing frameworks and security, browser security value and skills in cloud computing framework (SaaS), crucial cloud security service issues (PaaS), and cloud computing framework risk (IaaS). XML-Signature application and web services security are some technical issues in the cloud computing framework. Then, they suggest some possible solutions including raising the security of both web browsers and web service frameworks.

Furthermore, Kebande and Venter [18] were shedding light on some of the concepts such as obfuscating a botnet in a cloud environment to the Digital Forensic Readiness (DFR), which represents a proactive measure by collecting digital evidence and conservation have been used robots that is "a piece of non-malicious code deployed in stealth mode to infect virtual instances of computers for information harvesting. It is able to scan subnets, eavesdrop on activities over the network" in a way that is harmful to all for their willingness to digital forensic readiness. Kebande and Venter [16] point to the planning process of Digital Forensic Readiness (DFI) to face the threats and attacks in the cloud environment and detect malicious gaps in the cloud environment patterns. They suggest the provision of projects that support local communities to gain access to consumers via the cloud through hypothetical situations for PCs in the digital cloud.

It is important to consider privacy protection in cloud computing. Chen and Zhao [19] demonstrate that the possibility to access personal information through many websites like e-commerce is a serious issue in cloud computing. They suggest solutions such as providing a strong control on the information. Rai and Sharma [20] suggest three approaches to protect data in cloud computing. Encrypted data for privacy, redundant array of independent net-storages for privacy, and the Malaysian personal data protection act. Alshammari [21] proposes two suggestions to solve privacy concerns in cloud computing. First, web service security model (XML Signature and XML Encryption) to avoid restricted access – however, new web browsers should be developed because this model does not run with current web browsers. Second, the use of a trusted platform model to control security in a datacenter is not applied to the virtual environment – a virtual trusted model should be developed to run with the virtual environment.

In the military sector, Schear et al. [22] state that cloud computing offers substantial benefits to its users, through the capability to widely share information and enhanced security. Thus, the Department of Defense can get the advantages of cloud computing services. Consequently, the DoD seeks to utilize commercial cloud technology. Schear et al. [22] point out that combining services in a cloud test bed reduces risk for the DoD's acquisition of secure, resilient cloud technology by security evaluations and providing proofs of concept. The 2013 Defense Science Board (DSB) report of the Task Force on Cyber Security and Reliability in a Digital Cloud recommended that the "DoD should pursue private cloud computing to enhance mission capabilities, provided that robust security measures are in place" Evans and Grossman [23]. Per a Ministry of Communications and Technology [24], report: Saudi Arabia is looking for arrangements necessary to provide cloud computing services and controls. A decision was made to the implementation of controls to provide cloud computing services in Saudi Arabia, headed by the Ministry of Interior, Ministry of Post, the Royal Guard, National Guard, intelligence and other ministries.

To sum up, the study shows some of the challenges, security issues and privacy concerns facing cloud computing, and some technical problems. Also, it covered many suggestions and solutions to relieve the problems. It called for the use of cloud computing applications in open source software libraries to help in scientific research.

V. Conclusion

The performance of cloud computing can be improved if the security issues of cloud computing are identified well. Security problems are often storage based and network based. This research covered the most significant vulnerabilities and security concerns in cloud computing. It suggested some appropriate solutions to protect business and individual's data from attacks. This research performed a survey in the academic, commercial and medical sector in Saudi Arabia to find out to what extent cloud computing is implemented, to assess what its security problems are, and what user suggestions are to minimize the problems. Most of the responses from the survey noted that cloud computing requires new methods to secure remotely stored information while ensuring full

access for the owner. In general, the information security field is feeble in Saudi Arabia.

REFERENCES

[1] M. Peter and T. Grance, "The NIST definition of cloud computing," 2011.

[2] C. Bronk and E. Tikk-Ringas, "The cyber attack on saudi Aramco," *Survival*, vol. 55, no. 2, pp. 81-96, 2013.

[3] Wass. Monitoring electronic attacks on several government sectors, December 2016. [Online]. Available: http://www.okaz.com.sa/article/

[4] CITC. Report of the communications and information technology information and services, managed services center services cloud computing in saudi arabia. Technical report, CITC, 2015.

[5] CITC. Report on telecommunications and information technology sector of mobile telecommunications services in the kingdom of saudi arabia. Technical report, Communications and Information Technology Commission, 2015.

[6] Aitnews. 44th of May 2015. A study reveals the tendency of government sector institutions in Saudi Arabia to use the hybrid cloud in their IT. [Online]. Available: URL https://aitnews.com/

[7] B. Aljabr. Cloud computing and the possibility of analyzing and mining health data. (January 2012). [Online]. Available: http://www.alriyadh.com/698837

[8] B. H. Krishna, S. Kiran, G. Murali, and R. P. K. Reddy, "Security issues in service model of cloud computing environment," *Procedia Computer Science*, vol. 87, pp. 246-251, 2016.

[9] S. V Hatwar and R. K. Chavan, "Cloud computing security aspects, vulnerabilities and countermeasures," *International Journal of Computer Applications*, vol. 119, no. 17, 2015.

[10] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," in *Proc. the 2011 International Conference on Intelligent Semantic Web-services and Applications*, p. 12. ACM, 2011.

[11] H. Alshammari and C. Bach, "Administration security issues in cloud computing," *International Journal of Information Technology Convergence and Services*, vol. 3, no. 4, p. 1, 2013.

[12] M. Derfouf, A. Mimouni, and M. Eleuldj, "Vulnerabilities and storage security in cloud computing," in *Proc. 2015 International IEEE Conference on Cloud Technologies and Applications (CloudTech)*, 2015, pp. 1-5.

[13] D. Perez-Botero, J. Szefer, and R. B. Lee, "Characterizing hypervisor vulnerabilities in cloud computing servers," in *Proc. the 2013 International Workshop on Security in Cloud Computing*, pp. 3-10. ACM, 2013.

[14] M. Masky, S. S. Young, and T. Y. Choe, "A novel risk identi_cation framework for cloud computing security," in *Proc. 2015 2nd International IEEE Conference on Information Science and Security*, pp. 1-4, 2015.

[15] S. Ismail, et al. "Security issues and solutions in cloud computing-a survey," *International Journal of Computer Science and Information Security*, vol. 14, no. 5, pp. 309, 2016.

[16] M. Doinea and P. Pocatilu, "Security of heterogeneous content in cloud based library information systems using an ontology based approach," *Informatica Economica*, vol. 18, no. 4, p. 101, 2014.

[17] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *Proc. 2009 IEEE International Conference on Cloud Computing*, 2009, pp. 109-116.

[18] V. Kebande and H. S. Venter, "Obfuscating a cloud-based botnet towards digital forensic readiness," in *Proc. ICCWS 2015 the 10th International Conference on Cyber Warfare and Security*, 2015, pp. 434.

[19] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Proc. 2012 International IEEE Conference on Computer Science and Electronics Engineering*, vol. 1, 2012, pp. 647-651.

[20] A. K. S. Rai and S. D. Sharma, "Privacy issues regarding personal data in cloud computing," *International Journal of Advanced Research in Computer Science*, vol. 4, no. 11, 2013.

[21] H. Alshammari, "Privacy and security concerns in cloud computing," *International Journal of Computer Science and Information Security*, vol. 12, no. 3, p. 1, 2014.

[22] N. A. Schear, P. T. Cable, R. K. Cunningham, V. N. Gadepally, T. M. Moyer, and A. B. Yerukhimovich, "Secure and resilient cloud computing for the department of defense," *Lincoln Laboratory Journal*, vol. 22, no. 1, 2016.

[23] E Evans and R Grossman, "Cyber security and reliability in a digital cloud," US Department of Defense Science Board Study, 2013.

[24] The Ministry of Communications and Information Technology. Report: Saudi arabia looking for arrangements necessary to provide cloud computing services and controls. Technical report, MCIT, Saudi Arabia, October 2015. [Online]. Available: http://mcit.gov.sa/Ar/MediaCenter/Pages/MediaCenterNews.aspx

Amani M. Ghazzawi is a Teaching Assistant at Taif University, Saudi Arabia, in Management Information Systems department. She has been worked for a year as a responsible for the database at a charity in Saudi Arabia. She is now a master student in Computing Information Systems at King Abdulaziz University. She has accomplished some researches in Cloud Computing and E-commerce while her master thesis is in Data Mining and Decision Support Systems.

Fatimah M. Alqahtani is a Teaching Assistant at King Khalid University, Saudi Arabia. She is now a master student in Computing Information Systems at King Abdulaziz University. Fatimah has done some researches in Cloud Computing, Social Network Analysis and she looks forward to conduct researches in the field of Information Security.

Fahd S. Alotaibi is an Assistant Professor at the Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University. He obtained his PhD from the University of Birmingham, UK, in 2015. Dr. Alotaibi is interesting in several areas including Artificial intelligence, Natural Language Processing, Machine Learning, and Data Science.

Sjaak Laan, with more than more than 25 years of IT experience, is working with CGI since 2000 where he now works as a Principal IT architect in various markets. He is an expert on architecture, security and infrastructures, and has much knowledge of business processes, systems management processes and integration issues. Sjaak typically works as a lead architect or consultant in complex projects. Sjaak follows trends and developments in his field closely. Sjaak is Master Certified IT Architect (The Open Group) and TOGAF 8 and CISSP certified.