International Journal of Computing and Network Technology
ISSN (2210-1519)
Int. J. Com. Net. Tech. 6, No. 2 (May-2018)

http://dx-doi.org/10.12785/ijcnt/060205

An Analysis of Threats and Challenges in the Deployment of Cloud Computing

Ngo Yang Chong[1] and Humayun Bakht[2]

[1]*University of Warwick, Coventry, United Kingdom*
[2]*University of Warwick, Coventry, United Kingdom*

Received: 12 Jan. 2018, Revised: 20 April. 2018. Accepted: 25 April. 2018, Published: (1 May 2018)

Abstract: The rapid development of cloud computing has attracted a lot of companies stepping into the cloud family to enhance business efficiency. Cloud Computing is a computing model that enables far-reaching access to a shared pool of Information Technology (IT) resources such as storage, process power and network. However, adopting cloud service implies that businesses are giving away part of the control over information security to a third-party service provider. Also, the compatibility between cloud and on-premises IT system is a critical issue in the deployment of cloud. In order to gain a deeper understanding in the deployment of cloud, investigating the issues in cloud can escalate and improve the implementation process, hence, this study has examined the deployment threats and challenges in cloud computing through researching the current literature and industry report. This study has validated the security threat is still the top issue among various threats and challenges and data security is the ultimate concern in the usage of cloud computing. Since this study proposes a comprehensive view of the deployment threats and challenges in cloud computing, it can be used to facilitate the deployment process of cloud computing.

Keywords: Cloud Computing1, Cyber Security2, Network Security3.

1. INTRODUCTION (HEADING 1)

Cloud computing has been growing rapidly since Amazon brought this idea to the public. Mell and Grance (2009) defined cloud computing as 'a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction'. As cloud computing shares the hardware, processing power and data storage to the cloud consumer from the giant tech-companies such as, Microsoft, Amazon and Google, it carries the idea of sharing economy. The rise of sharing economy's idea boosts the development of company with the same idea such as, Uber, Airbnb, Kickstarter and of course cloud services companies. Although cloud computing improves the efficiency and effectiveness in business operations, the threats and challenges in cloud are the setbacks that lead to the inadequate cloud implementation or even failure deployment.

Companies are getting more experiences in security control as time goes by and becoming more confident in the usage of cloud in terms of information privacy. Therefore, management challenges such as cloud spending issue, integration process and Service Level Agreement (SLA) haveraised their attention in the deployment of cloud. Cloud spending issue is regarded as the top management challenge by the respondents. Although the security concern is the biggest challenge in cloud, the impact of other factors has been underestimated and lack of research especially regarding the management challenges. Since this study proposes a comprehensive view of the deployment threats and challenges in cloud computing, it provides a foundation for future research in terms of the issues in cloud computing. Rest of this work has been organized as follows. In section 2. Related work is presented. In section 3. Data Analysis is conducted. In section 4. Discussion and recommendations are covered whilst conclusion and future work are presented in section 5.

2. RELATED WORK

Moving to cloud gives corporation a huge cost driver that companies just need to pay for what they use instead of a substantial amount of up-front investment like the traditional IT system does. Cloud computing also provides the scalability according to different subscription plans and the agility to provision IT resources. However, adopting cloud service implies that

E-mail address: N.Chong.2@warwick.ac.uk, H.Bakht@warwick.ac.uk

businessesare giving away part of the control over information security to a third-party service provider. Also, the compatibility between cloud and on-premises IT system is a critical issue in the deployment of cloud.

It is easy to link with the data privacy problem when thinking of cloud computing. Actually, there are different kinds of issues and challenges during the adoption of cloud such as, security, availability, integrating with in-house IT and the ability to customize (Dillon, Wu and Chang, 2010). Investigating the threats and challenges and understanding all these problems are vital to a successful deployment of cloud computing. Currently, the major research about cloud computing issue focused on the security problem. There are lacking threats and challenges in the deployment of cloud in a general perspective. In the past few years, the security concern is the major challenge that affect the adoption of cloud computing. In 2018, security, cloud spending, expertise and control are the major challenges that face by the organisations with similar significance (RightScale, 2018). The challenges are no longer stressed on the technical issue which is security threat while they come in a management perspective such as control, expertise and cloud spending. An et al. (2016) indicated that each cloud deployment model provides different level of control, management and flexibility, thus, each model will have its unique deployment threats and challenges. As most of the companies are using on-demand service like cloud computing to improve business performance and efficiency, under the internet ecosystem, ensuring a smooth implementation of cloud computing is essential to the business operation and continuity.

Although cloud computing offers quite many benefits to its user especially for the business customer, there are several challenges of cloud such as, security, service level agreement, cost control, and cloud management have to be managed. The most significant challenge is the security issue which is agreed by different cloud researchers (Ali, Khan and Vasilakos, 2017; Caroll, Merwe and Kotzé, 2011; Martson et al., 2011; Dillon, Wu and Chang, 2010). Since using cloud will shift part of the business function to the internet, it is easier to be exposed to attack than traditional IT system (Popovic and Hocenski, 2010). In addition, the multi-tenancy and resource pooling characteristics have led to new security challenge that requires unique solution to deal with (Dillon, Wu and Chang, 2010). The security issue has been the major concern of the deployment of cloud computing since its first launch.

Apart from security challenge, Service Level Agreements (SLAs) is another major challenge in cloud computing . SLA is the agreement between cloud provider and customer which lists out the terms and condition for the cloud service. As cloud customers are moving part of the major business functions to the cloud, SLAs is essential to secure the service quality. The challenge appears when the provider and customer have different interpretations on the terms and lead to conflict regarding the cloud service (Dillon, Wu and Chang, 2010).

Cloud computing has a lot of advantages to enhance business efficiency while there are some major drawbacks that affect the deployment of cloud. The security issue is undoubtedly the most critical challenge in cloud computing as there is no companies can bear the data loss and privacy issues related to confidential information on cloud (Dillon, Wu and Chang, 2010). However, since companies become familiar and experienced in the use of cloud services, the concern over the security problem has been reduced and raised the concern over other deployment issues such as, SLA, cloud spending issue, lack of expertise, and governance (RightScale, 2018). This study addressed the threats and challenges in the deployment of cloud computing in a general perspective within a business organisation instead of focusing on a specific challenge or threat. The focus of the next section is on data analysis.

3. DATA ANALYSIS

A survey has been conducted targeting IT employees in order to get a broad understanding of cloud threats and challenges under the organisation point of view. As a result, this study interviewed five IT employees from different organisations and locations. This section analyses the data regarding three aspects which are threats, challenges and threats and challenges combined.

A. Threats related issues

This part analyses the survey result regarding the threats related issues in the deployment of cloud computing. Word R in the below given analysis represent respondent of the survey i.e. R1 respondent 1 etc.The majority of the respondents did not regard cloud as a threat to company information security, hence, it means that company has confident in the deployment of cloud service and able to mitigate security threat in cloud computing. 1 respondent recognised cloud service would be a threat to company information security as security issues still play a major role in the use of cloud service while 1 respondent was not sure as the security risk might be not as vital as before. In conclusion, company has a comparatively positive view on information security threats of cloud service.

TABLE I. COULD CLOUD COMPUTING BE A THREAT TO THE COMPANY INFORMATION PRIVACY/ SECURITY

Respondents	Answer
R1	No
R2	Yes
R3	No
R4	Maybe
R5	No

Data security and governance were selected the most as the significant security threats that both had been chosen by 4 respondents. They were following by network security which had 3 votes, and interfaces and virtualisation were chosen by 1 respondents each.

Data security was placed the most significant threat in cloud computing from 3 respondents while 2 respondents selected network security. Governance was the next threat after data and network security as it appeared in second place by R2 and R5, and third place for R4. Interfaces was appeared twice and placed as second place by R1 and R3. Apparently, data security is the most significant threats to company as company stores sensitive information on cloud. It is vital for company to make sure the data security to prevent any data leakage. The second significant threat is the network security which it is the most defenceless aspect in cloud because all the cloud service operation has to go through the internet which expose to the outside network and increase the chances of being attacked. Since there is lack of standards and measurements of cloud services, governance incurs a certain extent of threat in some respondents' view. Since interface is provided by the cloud service provider for consumer to manage and administrate the cloud service, users do not have the full control on the interfaces application and share the same interfaces with other cloud consumers, therefore, this exposes their security risk because of the multi-tenancy characteristic.

Compliance, legal and the credibility of cloud service provider (CSP) are selected by 4 respondents each. The abuse of cloud service was chosen by R2 only. Legal and compliance threats are similar in nature as they are rules and requirements have to be followed by the CSP and cloud consumer. Due to the increasing leakage or breach of confidential information such as Facebook massive data breach in 2018, compliance and legal have become another major threat apart from security. Credibility of CSP is critical as well since more and more companies are adopting cloud services, CSP may not provide the same level of service as before and threatening the service availability. R1 suggested an interesting threat which is the CASB configuration.

CASB is the abbreviation of cloud access security broker which is a software mean or service that locates between the cloud consumer's internal IT system and the CSP cloud system in order to play as a gatekeeper to enable the cloud consumers reaching the security control beyond their own infrastructure (Rouse, 2015). It is a security tool to help to encounter issues mainly visibility and data security as it provides practical approach to manage the sensitive data and ensure the compliance with cyber security regulations and polices (Bitglass, 2014). The configuration of CASB creates an extra layer of threat as there is one more party involved in the cloud ecosystem and the CASB is accessible to the information transferred between CSP and cloud consumer. There were 4 of the respondents agreed with the deployment threats are the nature of cloud computing. The nature regards cloud computing characteristic, enabling technologies and roles. R4 was not sure about this question.

TABLE II. THREATS OTHER THEN SECURITY ISSUES

Respondents	Answer
R1	Legal, Credibility of CSP, others: (CASB configuration)
R2	Compliance, Legal, Credibility of CSP, Abuse of cloud service
R3	Compliance, Credibility of CSP
R4	Compliance, Credibility of CSP, Legal
R5	Compliance, Legal

B. Management challenges

This part analyses the survey result regarding the cloud challenges in the deployment of cloud computing.

Integration with in-house IT, SLA and Lock-in service are the major challenges as they got 4 votes each. Following these three challenges, managing cloud spending is also regarded as the challenges in cloud deployment by 3 respondents. Lacking expertise and loss control over IT system had 1 vote for each. R1 suggested a specific challenge which was the upgrade process of cloud computing. The upgrade process is challenging nowadays since the competition among CSP is intense, therefore, it leads to a frequent upgrade to enhance cloud service and cause the fluctuation of service availability (Neamtiu and Dumitras, 2011). Managing the upgrade process can cause quite many troubles as there will be a downtime during the upgrade.

TABLE III. CHALLENGES IN THE DEPLOYMENT OF CLOUD COMPUTING

Respondents	Answer
R1	Integration with in-house IT, Lock-in service, Others: (Upgrade process)
R2	Managing cloud spending, SLA, Loss control over IT, Lock-in Service
R3	Managing cloud spending, SLA, Integration with in-house IT
R4	Managing cloud spending, SLA, Lack of expertise, Integration with in-house IT, Lock-in service
R5	SLA, Integration with in-house IT, Lock-in service

R2, R3 and R4 chose managing the cloud spending as their top challenge while R1 chose upgrade process and R5 chose SLA. Managing cloud spending was regarded by the majority as the top challenge as the spending on cloud might be higher than we thought. It is because the cost could be multiplied by choosing the unsuitable subscription plan and all kinds of miscellaneous fees. In a long term, it might cost higher than the traditional IT system, therefore, managing the cost of cloud computing is regarded the top challenge by 3 respondents. SLA was chosen the top challenge by 1 respondents while another 3 respondents chose SLA as second place or third place. SLA is also a challenging issue in cloud as there is no standardised regulation or practice could be followed, the SLA acts as a key role for both CSP and consumer to stick to, hence, SLA is vital to the successful deployment of cloud service to avoid dispute.

R1, R2 and R4 considered the challenges are tended towards technical in cloud. R1 stated that the integration of poorly managed upgrades would be a problem. This relates to the integration with in-house IT and upgrade process. R1 stressed on the control over the IT system as "When you do not have 100% control end to end". It means that the integration and upgrade are easily gone wrong without full control on the process as there are quite many issues dealing with CSP and external parties to complete the cloud deployment. R2 and R4 both regarded the technical issues as the challenge because of the advancement of technology. R3 thought that it was a management challenge because of the credibility of CSP. R3 expressed "The cloud service provider is not always reliable", hence, it relates to the management between CSP and consumer rather than the technical aspect in cloud. R5 considered cloud challenge was more towards on management because the standards on technical aspect were different within different CSP, hence, it would be a management issue on managing the cloud service rather than the technology itself.

C. Regarding both threats and challenges in cloud computing

This section relate to the threats and challenges in cloud computing as a whole. The majority of respondents agreed that the advancement of technology would lead a relatively manageable cloud environment than before. R2 was not sure and R5 disagreed on this question.

The majority of respondents considered security would still be the biggest challenge at the moment, while 2 of the respondents regarded other factors would be the biggest challenge which were integration and upgrade issues, and the cloud readiness. R2, R3 and R4 thought security as the biggest challenge had a common view that the information security would be getting more challenging. R4 expressed as "as the development of society……., and it will encounter more challenge to protect the information not to leak", as it reflected that the development of the world would to lead a more complex situation for companies to tackle data security issues. Also, R3 expressed "the data was not controlled by company and having the risk to leak the data. This showed that company was still afraid of the uncontrollable environment in cloud computing, hence, the sensitive data in the cloud would be a huge risk in the deployment of cloud computing. R1 considered the integration and upgrade in cloud would be the biggest challenge and claimed, "cloud companies spend a lot more on security because it is a key to success". Even though R1 regarded integration and upgrade would be the main issue, he still expressed the view on cloud security that having a dedicated security control in cloud is a key to success. R5 brought up an interesting point on the cloud readiness of firms. He mentioned "Security won't be a big issue……, cloud readiness is the greatest challenge because company lacks expert and framework to adopt cloud at this stage". He viewed that the cloud security issues would not be a big problem as long as there was a security team to control whilst the cloud readiness of company regarding the expert and framework in cloud service were the biggest challenge at the moment. As a result, lacking expertise and foundation of cloud were the key challenge to success.

D. Discussion

Respondents had given different views on the threats and challenges in the deployment of cloud computing. Regarding the first part which relates to the threats in cloud computing, the majority of the respondents do not think cloud computing will be a threat to company information security. It shows that the respondents are confident with the use of cloud computing service while

the majority of them agree the security threats are the nature of cloud computing. Data security is the biggest concern from the survey result and following by network security and governance. In addition to security threats, compliance, legal and credibility of CSP are also other concern regarding cloud threats.

TABLE IV. KEY FINDINGS FROM THE SURVEY RESULT

Key Findings
Companies are confident in the use of cloud service regarding the information privacy and security even though they mostly agree the security threat is the nature of cloud computing. Data security is the biggest concern among various threats.
The cloud spending issue is the leading concern in companies. SLA and integration challenges are also significant to companies in a relatively lower extent. Challenges are tended towards on the technical aspect as cloud computing comprises complex technologies.
The improvement in technology will assist the deployment of cloud service and security will still be the main issues in cloud apart from emerging threats and challenges. Upgrade and integration, cloud readinesses are other key issues as suggested by respondents.

In respect of the result in cloud challenges, managing the cloud spending is the biggest challenge. It is following by the SLA issues and integration issues. The majority of respondents viewed that the cloud challenges are more inclined to the technical issues as the integration and upgrade process incur technical problem as well as the more data or information the company handles, the more technical control is required on the cloud service.

Respecting to the cloud computing deployment threats and challenges altogether, respondents agreed the technology advancement will benefit to the management of cloud service and able to mitigate the related risks. The security will still be the major concern for the majority of the respondents as this is an unavoidable issue in the information age that there will be more and more sensitive data managed on cloud.

Undoubtedly, security concerns will still be the major concern especially for data security as the data is growing faster than ever before and every person will generally approximately 1.7mbs of data every second of the day (Zhou, 2016), hence, data security will stay as the top threat in cloud. Even though other threats such as network security, governance and interfaces are vital as well, these threats imply the impact to the data security behind different comprised technologies in cloud. Therefore, the prominence of data security is unshakable. Also, the regulation on data security is changing time to time especially the newly introduction of GDPR. The compliance issue will become complicated because of the new regulation and increasing numbers of involved parties. Besides, management challenges are crucial in nowadays cloud computing as it affects the effectiveness, cost and management of the cloud system. As companies viewed cloud spending issue as the top challenge, it showed that they encountered costing problem while using cloud services and unable to identify suitable solution to decrease the cost of cloud. Since the subscription plan is a relatively a new pricing model for businesses to adopt IT services, it takes time to evaluate the spending pattern and the cost-effectiveness. It is possible to spend more than a traditional IT system because of the complicated cost structure (Bridgwater, 2017). Likewise, integration has been regarded as another importance challenge as the integration process implies the element of SLA, upgrade process and governance. Integration will become more complex than ever before no only because of the interoperability issue internally, but also between cloud to cloud. Ashok (2018) stated that in 2019, companies tend to adopt a hybrid-cloud approach that provide an advanced cloud solution to enhance efficiency and effectiveness. In addition, since the advancement of technology will assist the deployment of cloud computing, how to manage the cloud service as its optimal state is decisive in the future. However, there is an obvious lack of research in the field of management challenge of cloud computing while the current literature targets on the security issue which are technical based.

4. RECOMMENDATIONS

This section discusses the key findings from the data analysis followed by recommendations regarding the discussion on cloud computing threats, challenges and threats and challenges as a whole.

A. Cloud Copmuting Threats

Since the cloud computing has been introduced for 12 years (Regalado, 2011), companies are getting familiar with this disruptive technology and becoming confident in the use of cloud services as reflected in the survey. Organisations were mostly confident in the use of cloud despite the threats to company's information privacy. Data security is the most significant threats in cloud security. This validates the literature research that data security is the ultimate threats to company's security. Although companies recognise the security threats are the nature of cloud computing which is inevitable, it is possible to omit the issues by a better cloud planning. Also, companies regard data security as the biggest concern in the deployment of cloud, but it appears to be not as important as before since some of the companies regard network security and governance are others top threats in cloud. Apart from the security threats, compliance, legal and the credibility of CSP are also some major concerns in cloud services. CASB configuration was regarded as cloud threats by one respondents, but

there is no current literature discussed this issue because it is a relatively new topic in the cloud ecosystem.

Recommendation regarding cloud computing threats

Since organisations are familiar with the use of cloud services, security threats are no longer as important as before like the current literature stressed on. Governance, compliance, legal issues, CASB configuration are other key threats as reflected in the survey. The future work in cloud computing threats can be focused on theses aspects rather than the technical threats.

B. Cloud Copmuting Challenges

Cloud spending problem is the greatest concern among respondents and following by SLA and integration challenges. One respondent has stressed on the issue in integration and upgrade process of cloud while others have mentioned in a relatively lower extent. Since the companies' cloud challenges are agreed to be distinct mostly, the integration process is different from company to company as well as the lack of standards and regulations. Different cloud service providers have different approaches and system for integration, therefore, the interoperability issue is very likely to become the major concern in the future because of the increasing numbers of cloud service providers, consumers, and regulators. The collected data validated the SLA is a key issue in cloud, however, cloud spending is viewed as the top critical challenge.

Recommendation regarding cloud computing challenges

Since there are relatively insufficient research on the cloud computing management challenges compare to security issues in cloud, it needs further research regarding different issues in management challenges. Although SLA is viewed as the top challenge by the current literature, from the result of the data analysis, cloud spending problem is regarded as the top critical issue and other challenges such as integration and upgrade process require additional research as well. Also, CASB is also a new role in cloud ecosystem which lacks study. Challenges relates to CASB can be done for future research as well. Apparently, cloud spending issue needs an in-depth research as the costing issue will become a complex structure as companies increase their cloud usage from 1 cloud to several clouds.

C. Cloud Computing Threats and Challenges

This study also has validated the security threats will still be the biggest challenge as most of the researchers' confirmed. Also, the threats and challenges are tended to technical issue which validated the current research as well. However, apart from the security challenges, which are regarded as technical issue, management challenges such as, integration, upgrade process and cloud readiness are regarded as the biggest challenge by few companies. This reflects that although technical issue is critical to cloud deployment, management issues may affect the implementation as well which cannot be underestimated.

Recommendation regarding cloud computing threats and challenges

Although the security threats are still the biggest issue nowadays, growing concerns of other challenges are needed to be addressed as well. In general, cloud computing deployment threats and challenges require a more in-depth research regarding different issues instead of the emphasis on security threats. In long term, a framework or guideline addressing deployment threats and challenges in cloud computing could be suggested in order to adopt a successful cloud service. In specific, the framework or guideline is ideally geographical based as the rule and regulation on information privacy are distinctive in different locations, therefore, the threats and challenges may vary as well.

5. CONCLUSTION AND FUTURE WORK

This work has investigated threats and challenges in the deployment of cloud computing. Research findings of this paper reveal that data security remains importance in cloud computing for possibly a longer period of time. It still needs a lot of research effort to tackle the data security threat as well as the compliance challenge on data regulation. These two aspects are still needed continuous research. Apart from the securityproblems, management challenges in general require a comprehensive research especially on the spending issue. There areonly limited literatures discussed the cloud's costing issue regarding Return on Investment (ROI) as the cost of Cloud Computing is still a new form of cost structure to businesses. An evaluation framework can be built to address the spending issue and avoid over spending for corporations. A future research can be conducted to investigate the management challenges and security threats in cloud computing within a specific region or country.

ACKNOWLEDGMENT

Research findings as presented in this paper are the result of the MSc dissertation project entitled "Investigating Threats and Challenges in the Deployment of Cloud Computing" conducted at the University of Warwick under the supervision of Dr. Humayun Bakht.

REFERENCES

[1] Ali, M., Khan, S. U. and Vasilakos, A. V. (2015) 'Security in cloud computing: Opportunities and challenges', Information Sciences. Elsevier Inc., 305, pp. 357–383. doi: 10.1016/j.ins.2015.01.025.

[2] An, Y. Z., Zaaba, Z. F. and Samsudin, N. F. (2016) 'Reviews on Security Issues and Challenges in Cloud Computing', IOP Conference Series: Materials Science

and Engineering, 160(1), pp. 0–9. doi: 10.1088/1757-899X/160/1/012106.
[3] Ashok, A. (2018) Four Trends In Cloud Computing CIOs Should Prepare For In 2019, Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2018/07/05/four-trends-in-cloud-computing-cios-should-prepare-for-in-2019/#cd46e294dc2e [Accessed: 18 August 2018].
[4] Bitglass. (2014) The Definitive Guide to Cloud Access Security Brokers. Bitglass. [Online]
[5] Bridgwater, A. (2017) The complicated cost of cloud, Raconteur. Available at: https://www.raconteur.net/technology/the-complicated-cost-of-cloud [Accessed: 18 August 2018].
[6] Dillon, T., Wu, C. and Chang, E. (2010) 'Cloud Computing: Issues and Challenges', 2010 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 27–33. doi: 10.1109/AINA.2010.187.
[7] Popovic, K. and Hocenski, Z. (2010) 'Cloud computing security issues and challenges', MIPRO, 2010 Proceedings of the 33rd International Convention, pp. 344–349.
[8] Mell, P. and Grance, T. (2009) 'The NIST Definition of Cloud Computing', National Institute of Standards and Technology, 15, doi: 10.1136/emj.2010.096966.
[9] Neamtiu, I. and Dumitraş, T. (2011) 'Cloud software upgrades: Challenges and opportunities', in 2011 International Workshop on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems, pp. 1–10. doi: 10.1109/MESOCA.2011.6049037.
[10] Regalado, A. (2011) Who Coined 'Cloud Computing'?, MIT Technology Review. Available at: https://www.technologyreview.com/s/425970/who-coined-cloud-computing/ (Accessed: 9 August 2018).
[11] RightScale (2018) 'RightScale 2018 State of the Cloud Report', pp. 1–31. Available at: http://www.rightscale.com/lp/2015-state-of-the-cloud-report.
[12] Rouse, M. (2015) 'What is cloud access security broker (CASB)?' Availableat: https://searchcloudsecurity.techtarget.com/definition/cloud-access-security-brokers-CABs (Accessed: 6 August 2018).

Mr. Ngo Yang Chong
Mr. Chong is a master student in Msc of e-Business Management at the University of Warwick. He obtained his bachelor's degree in business administration from the Hong Kong Shue Yan University. He is interested in business transformation and the use of technologies under business's objectives. More specifically, his work examines the adoption of various technologies in a business context.

Dr. Humayun Bakht
Dr. Bakht is an Academic Advisor/ MSc dissertation supervisor at the University of Warwick. Dr. Bakht is a regular contributor of both academic and non academic articles. He has also authored several books including 'Mobile Ad-hoc Networking' and 'A Roadmap to PhD'.