Emerging Technologies and Cyber Risk: How do we secure the Internet of Things (IoT) environment?

Charla Griffy-Brown
Pepperdine University

Demetrios Lazarikos
Blue Lava Consulting

Mark Chun
Pepperdine University

Cloud computing and the Internet of Things (IoT) have transformed businesses, enabling agile and cost-effective IT infrastructure. The challenge is that these new opportunities create a co-mingled architecture which is difficult to secure. The complexity of this architecture is magnified with the IoT. Based on interviews with executive leadership teams and boards of directors facing these new environments, we developed the over-arching research question: How do we secure increasingly dynamic architecture in an environment while supporting and creating agile business growth? We then narrowed this down to more specific questions dealt with in this study. The research involved an in-depth exploration of this problem using a survey instrument and multiple qualitative methods involving business leaders from 59 companies between 2017 – 2018. Based on this analysis, we developed an information security framework for executives in this new environment that builds on previous work. This framework is called the Extended Risk-Based Approach and provides businesses with an approach for securing an enterprise amidst the IoT and agile architecture. Importantly, the data analyzed suggests that this approach is critically needed to address the rapidly growing complexity of enterprise architecture and the digital world we live and work.

INTRODUCTION

As the Internet of things (IoT) becomes integrated into firms' go to market strategy to support the business, it is critical for executives, IT specialists, and Cyber Security practitioners to understand how IoT impacts their cyber risk. IoT solutions introduce threats to corporate data and systems that have not been considered before. Therefore, it is essential that executives, board members and business leaders be aware of the security risks with IoT solutions as well as how to address them.

A number of widely publicized attacks (Ranger 2017) have left business leaders with the impression that the IoT is less secure than existing enterprise architecture. What often goes unmentioned is that most attacks originate because of failures to implement basic protections. Companies often implement new

technologies for business growth without taking a pro-active risk-based approach as part of a cyber-security posture.

Another challenge is that IoT-enabled devices (particularly industrial IoT) are typically deployed in high traffic areas such as the factory floor, public thoroughfares, stores, vehicles, offices, or homes. That means that they are often physically accessible by employees and even the general public. If we compare that to modern cloud data-centers, where access is severely restricted, there is a significant vulnerability difference even from a physical access perspective. More people with access increases the risk of compromise, so it is critical to evaluate risk accordingly.

Just as in the case of any technology deployment, these obstacles are surmountable. The question is really *how* to *proactively* implement security measures. This may not require a new approach to cyber security or risk but instead that practitioners build on an existing foundation. Therefore, the primary research questions for this investigation were: Have there been changes in the adoption of a risk-based approach? What level of executive oversight is involved and how does this impact budgeting? Is there a new framework that needs to be applied and what would this look like? What thematic recommendations are there for securing IoT?

Previous research in this area resulted in the development of the Risk-Based Approach. The high-level security framework used for this study was developed and validated with Fortune 500 companies and is referred to as the Information Security Maturity Model (Figure 1) with the final column being the Risk-Based Approach (Griffy-Brown, et. al. 2016).

FIGURE 1
THE INFORMATION SECURITY MATURITY MODEL

Source: Griffy-Brown, Lazarikos, and Chun 2016

This model explains that over time companies can move from a reactive state in information security to a proactive state. The first column, called "Blocking and Tackling" refers to a completely reactive environment. In this environment, there is often a lack of support, underfunding, lack of staff and lack of metrics for understanding what is happening with respect to information security. The next column, called "Compliance Driven", refers to a corporate environment in which a control-based approach is taken but this is driven by audit and regulation rather than positioning for emerging threats. The final column called "the Risk Based Approach" refers to companies which are using big data and behavioral analytics and linking events across disciplines to understand and position themselves for potential threats. In this approach, businesses have a risk framework in place, and are using dynamic controls, metrics and processes aligned with the business.

The current research first will identify what emerging technologies the companies examined are presently working with in order to provide a context for IoT. Then we will look at whether a Risk-Based

Approach is currently a part of the budgeting process and if executive oversight is now required. Finally, based on focus group discussions with business leaders and decision-makers, we will present the Extended Risk-Based Approach developed for IoT based on these discussions. Using these results, critical considerations moving forward are presented in order to advance our understanding and ability to position business for agile growth while addressing information security challenges such as IoT.

The structure of this paper develops the logic above. The next section will identify gaps in the literature and present theories that might help us holistically understand the IoT cyber risk challenge and support agile business growth. Following this, the results of the survey instrument will be presented addressing the first two research questions. The final section will explain solutions for executives and IT practitioners and expand the meaning of this research in terms of scholarly theory and further exploration. Based on this analysis, companies can similarly use the security framework presented as a tool for advancing further real-world solutions to address IoT security challenges. Scholars can begin to apply systems dynamics theory and develop greater insight and tools.

GAPS IN THE LITERATURE AND PROPOSED THEORY

The cyber security literature research primarily focusses on requirements and solutions for requirements (Honer 2013). In this regard, research on Attack/Harm Detection is prolific (Chonka and Abawajy 2012; Chonka et. al. 2011; Monfared and Jaatun 2011). Non-repudiation is widely discussed and cited (Nishikawa et. al. 2012; Kumar and Sburamanian 2011; Chou et. al. 2011) and Security Auditing has been deeply explored (Deshmukh et. al. 2012; Gul et. al. 2011; Munoz et. al. 2012). By far the most researched topics are privacy, confidentiality, access and control (Chen et. al. 2013; Cho and Lee 2012; Llanchezhian et. al. 2012; Elham and Lebbat 2012; Zhu and Wen 2012). In his extensive literature review of the information security scholarship over the last decade, (Honer 2012) identifies these areas as the topics most scholars are examining. However, in the applied business world, these issues are never dealt with in isolation and there is a need for broader thinking given the new agile architecture more companies are using.

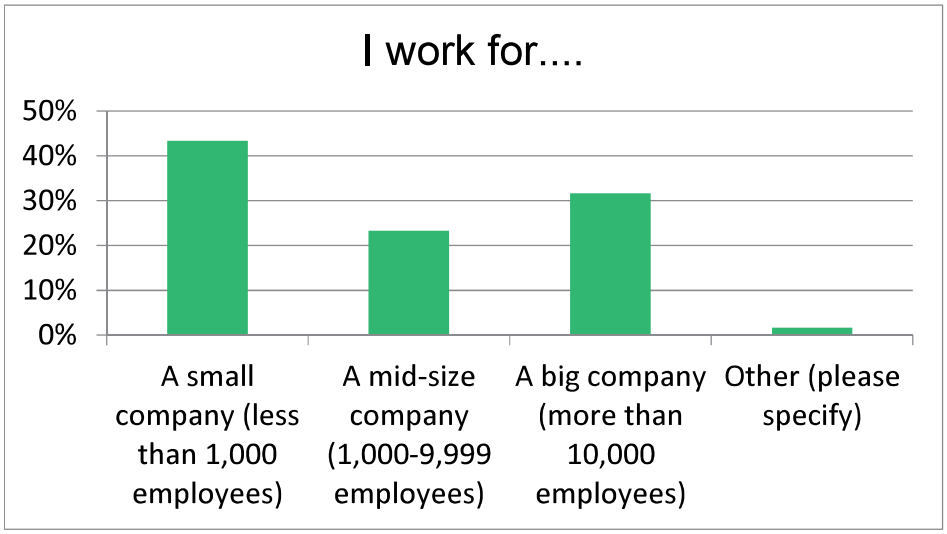
An overarching theory is required to enable scholars and practitioners to think about and address the security challenge from a holistic perspective (Ryan and Watson 2017). Methodologically, researchers have recommended three potential theoretical approaches including Game Theory (Chen et. al. 2011), Fuzzy systems theory (Wang et. al. 2016) and Graph Theory (Yao et. al. 2013) to address IoT security. Unfortunately, these approaches are tools that could be used within a system to identify and possibly address vulnerabilities but not a holistic theoretical framework to shape thinking. Two theories that show promise are General Systems Theory (GST) and Systems Dynamics (SD) Theory. GST is based on biological systems and is used across disciplines to describe systems that exhibit unpredictable behavior occurring as a result of non-linear spatio-temporal interaction among sub-systems (Von Bertalanffy 1968). Systems Dynamics models systems behavior based largely on the time-trajectory of system variables (Forrester 2007).

This research will seek to see which theoretical approach resonates more with business leaders and business processes. The next step beyond theoretical evaluation is identifying an applied framework for businesses that connects with theory and to design a quantitative evaluation. Through the research questions and case methodology we initially explore a systematic applied approach to scaling, particularly a mixed legacy, virtual and third party eco-system that is continuing to build-out using emerging technologies. The theory can inform the design of the applied approach. This research fills a much needed gap building on work published regarding the Risk-Based Approach (Griffy-Brown et. al. 2016). It also provides an evolving theory and framework for exploring and securing this new dynamically developing environment.

METHODOLOGY

The data collection strategy used in this investigation first involved the collection of empirical data collected from 59 firms across 12 industry verticals and including small businesses as well as large businesses (Figure 2). From these firms executives and business leaders were asked for interviews.

FIGURE 2
SIZE OF BUSINESS SURVEYED



In addition, the business leaders who responded were from across the organization but had high-level responsibilities within their organizations (Figure 3).

FIGURE 3
DECISION-MAKING LEVEL OF RESPONDENTS

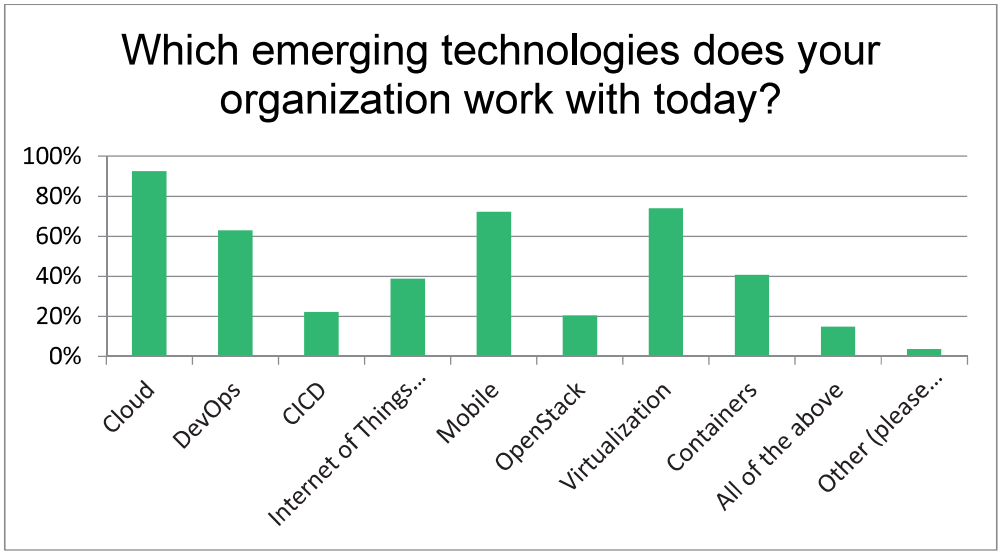
The second data collection technique used was qualitative and is known as triangulation. This involved multiple methods for collecting historical and longitudinal data (Yin 1994; Strauss and Corbin 2015). Multiple sources of data such as participant observation, open / structured interviews were

collected through structured and semi-structured interviews with business leaders from August 1, 2017 to January 1, 2018. Coding included highlighting issues that appeared more than 8 times in the interviews as part of the construct and to develop the framework for analysis as well as the recommended solutions. The qualitative methodology employed helped this research to gain an understanding of the business leader's perceptions and concrete solutions. It also enabled us to identify the key common problems, and to understand how to address these problems through dynamic and agile methods. The names of organizations have been kept confidential and anonymized in the reporting of the results, particularly given the sensitivity of the information security area.

RESULTS – EMERGING TECHNOLOGIES AND USE OF THE RISK-BASED APPROACH

The survey revealed that IoT is an emerging technology with deployment across different firms regardless of size. It also revealed that cloud, virtualization, development operations, and mobile are all very much still at the forefront of enterprise architecture considerations (Figure 4).

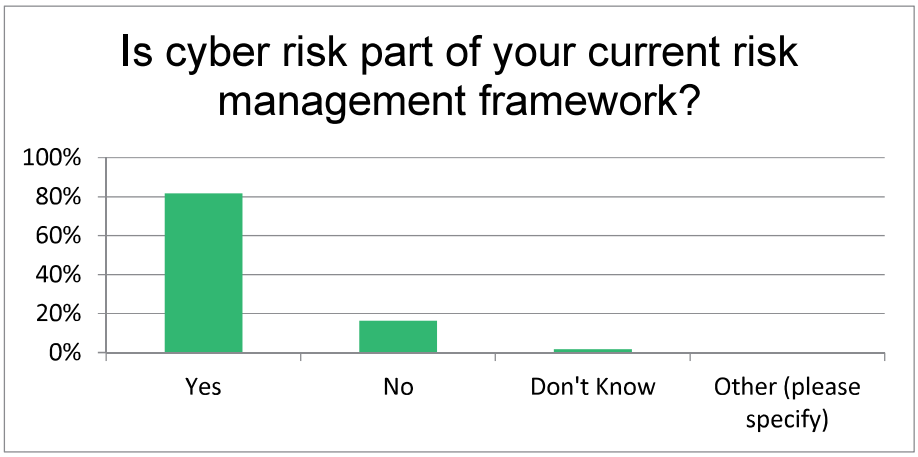
FIGURE 4
THE EMERGING TECHNOLOGIES FIRMS ARE WORKING WITH CURRENTLY



That being said, 39% of the companies surveyed were working with IoT. As enterprise architecture, driven by increasing needs for agility, continues to evolve with these emerging technologies all interwoven, it becomes important to understand how to secure this dynamically changing environment [2]. The question is: Does this involve the Risk-Based Approach?

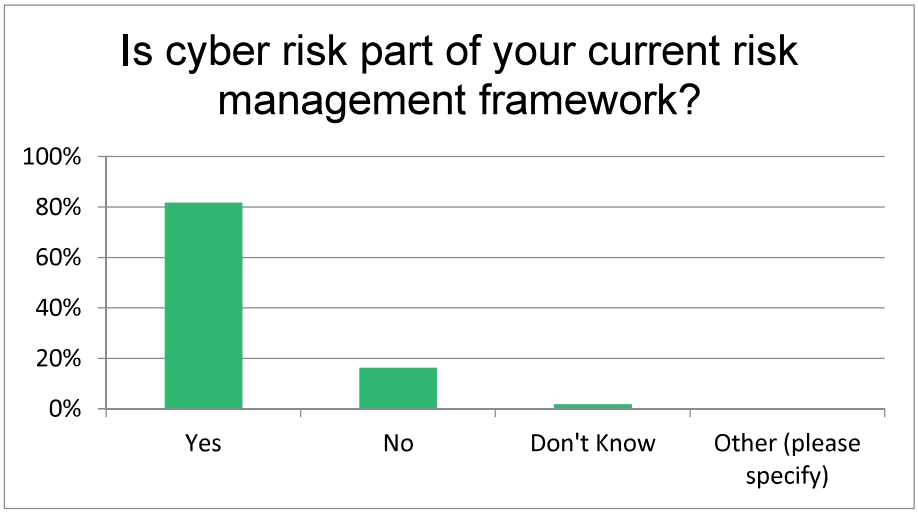
Surprisingly, 80% of the companies surveyed indicated that the Risk-Based Approach was now a part of their budgeting process (Figure 5). This is a significant change from 2016 when 40% of companies surveyed used the Risk-Based Approach and the vast majority were simply compliance driven [2].

FIGURE 5
CYBER RISK AS PART OF THE MANAGEMENT FRAMEWORK



What is even more significant is the elevation of cyber risk to the board level (Figure 6). Nearly 65% of the respondents replied that the board was involved in their cyber security oversight.

FIGURE 6
BOARD OVERSIGHT FOR CYBER SECURITY



Given these changes in oversight, the growth of cyber risk as part of the management process, and the continued growth of agile architecture including IoT, is a different security approach called for?

THE EXTENDED RISK-BASED APPROACH FOR IOT

Executives and business leaders were presented with the foundations of GST and SDT to consider and asked which best described IoT and could provide insight into how to address security? Universally, GST, which describes concepts largely from an organismic biological perspective, was too abstract. Systems Dynamics Theory, with a focus on modelling relationships between various systems, was viewed as more applicable to this problem and current business processes. IoT was envisioned by leadership as less of an "ecosystem" than a "system of systems". Furthermore, decision-makers felt SD could be modelled at different levels. The uppermost level would be the IoT core infrastructure. The next level

would be individual application areas such as healthcare, energy, or industrial IoT. At the lowest level, SD would model IoT agile or waterfall project management optimizing these business processes. Given the existing SD modelling of agile software development, connecting the theory to a Risk-Based Approach was a natural leap in business thinking.

Building on this theoretical understanding, the executives and business leaders who were a part of the qualitative research felt that an entirely new approach was not required, but instead an extension of the risk-based approach was suggested. This was important because of the rapid change in emerging technologies which were being incorporated and then exiting the architectural landscape. Therefore, an approach which would extend risk beyond project development throughout the device life-cycle was suggested. The Extended Risk-Based Approach which resulted is demonstrated in Figure 7.

FIGURE 7
EXTENDED RISK-BASED APPROACH: SECURING EVERY DEVICE THROUGHOUT ITS LIFE-CYCLE

In this framework, in addition to the Risk-Based Approach described in earlier research, every device would follow a process for risk evaluation throughout its life-cycle. This would be linked to budgeting and the ongoing security posture of the firm. This Extended Risk-Based Approach would create a risk eco-system as enterprise architecture develops. The advantage is that budgets are built with life-cycle risk in mind as well as the interaction of cyber risk exposures in an ecosystem. This would be coupled with and amplify the user-behavior analytics and cross-discipline monitoring which is part of the original approach. Furthermore, this approach builds on the SD theory, potentially incorporating risk into the modelling of the relationships all three levels described earlier.

From these discussions, themes emerged, and the following recommendations for securing IoT were developed:

1. **Take an Extended Risk-Based Approach**: As discussed, cyber-security best practices follow a risk-based approach that considers both the ease of an attack and the impact when one happens. What is required is an end-to-end risk evaluation through the device life-cycle coupled with proactively building risk into budgeting.
2. **Be Data-centric**: IoT data is characteristically heterogeneous, often introduces inaccuracy, is massively real-time, and introduces semantic issues. Data indexing and protection must be

considered with respect to national and international regulations at each stage of project development. Methods for sampling continuous data and querying semi-structured data will need to be developed and deployed. Limiting, segmenting, or isolating the IoT devices that connect to each other can assist in analytics and limit the damage should a breach occur. This can also be addressed by maintaining control over the business IoT infrastructure. The risk is owned by an individual business unless it is intentionally transferred. This starts with device selection so make sure that devices have the security features needed and, even more importantly, that the data can be analyzed by the company that owns the risk.

3. **Don't forget the basics:** Always leverage existing expertise and processes applying proven security technologies, tools, and best practices already known and used extensively. This includes the evaluation of risk that businesses in this study are already using to budget for cyber-attacks. In many cases, existing processes and tools can be implemented directly. Companies can restrict what IoT devices can do and what they communicate with, they can add encryption, and add monitoring mechanisms. This doesn't mean that in some cases, such as micro-controllers and low-power networks, businesses won't need to apply new techniques. They will. However, it is essential firms build on existing principles and concepts. Cyber security is not just a technology problem but a people, process and risk problem.

IoT adoption is still emerging as evidenced by the data presented in this research. Therefore, there aren't many established standards yet even as the number of devices brought to market is quickly rising. Given that these standards are emerging, tracking and adhering to standards developed by ISO, IEEE, ITU and others, as they evolve, is also critical. As a result of these emerging systems dynamics, there is a strong need for adopters to carefully plan and build in security throughout the life-cycle of a device as indicated by the Extended Risk-Based Approach presented here.

CONCLUSION

This research explored the further development of agile architecture with IoT and the implications for cyber security. In particular, the focus was on examining what is happening in business to provide a practical approach for business leaders to follow in securing this new interconnected digital landscape. This work identified the need for a holistic theoretical approach that resonated with business practice. Decision-makers felt that Systems Dynamics Theory would be more helpful than General Systems Theory and that it connected well with the Risk-Based Approach. Furthermore, future empirical work should be designed and tested to validate and describe this connection. The quantitative results showed that more businesses are taking a Risk-Based Approach with greater oversight coming from the board level. It also showed that IoT was still in the early stages of deployment. The qualitative research built on these results to develop an extended approach through conversations with business leaders that would help companies continue to meet the challenges of cyber-security with IoT. The Extended Risk-Based Approach, now added to business portfolios, was coupled with some very specific recommendations from business leaders. Ultimately, addressing cyber security requires both process and leadership as businesses continue to strategically adopt emerging technologies.

REFERENCES

Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2011). XRM – IoT: A trust management model based on fuzzy reputation for internet of things. *Computational Science Information Systems*, 8, 1207-1228.

Chen, G., Miao, J., Xie, F., & Mao, H. (2013). A framework for storage security in cloud computing. *Journal of Management and IT*, 3(2), 87-97.

Cho, G. H., & Lee, S. A. (2012). *A secure service framework for handling security critical data on the public cloud*. Guangzhou, China.

Chonka, A., & Abawajy, J. (2012). *Detecting and mitigating HX-DoS attacks against cloud web services*. 4th International CSS Symposium, Melbourne, Australia.

Chonka, A., Xiang, Y., Zhou, W. L., & Bonti, A. (2011, July) Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications*, 34(4), 1097-1107.

Chou, Y., Levina, O., & Oetting, J. (2011). *Enforcing confidentiality in a SaaS cloud environment*. 19th Telecommunications Forum (TELOR) Proceedings, Belgrade, Serbia. pp.90-103.

Deshmukh, A. A., Mihovska, A., & Prasad, R. A (2012). *Cloud computing security schemes:- TGOS and TMS.* Information and Communication Technologies (WICT), 2012 World Congress. Trivandrum, India. Oct. 30, 2012-Nov. 2 2012, 203-208.

Elham, H., & Lebbat, A. (2012). *HX-DoS attacks against cloud web services*. Melbourne, Australia.

Forrester, J. W. (2007). System Dynamics – a personal view of the first fifty years. *System Dynamics Review*, 23, 345-358.

Griffy-Brown, C., Lazarikos, D., & Chun, M. S. (2016) How Do You Secure an Environment Without a Perimeter? Using Emerging Technology Processes to Support Information Security Efforts in an Agile Data Center. *Journal of Applied Business and Economics*, 18(1), 90-102.

Gul, I., Ur Rehman, A., & Islam, M. H. (2011, June 21-23). *Cloud computing security auditing*. Gyeongju, Korea, pp. 143–148.

Honer, P. (2013). *Cloud Computing Security Requirements and Solutions: A Systematic Literature Review*. Thesis. University of Twente, Faculty of Engineering and Mathematics and Computer Science. Enschede, Netherlands.

Kumar, P.S., & Sburamanian, R. (2011, October). Homomorpic Storage Secruity in Cloud Computing. *Information International Interdisciplinary Journal*. 14(10), 3465-3476.

Llanchezhian, J., Varadharassu, V., Ranjeeth, A., & Arun, K. (2012). *To improve the current security model and efficiency in cloud computing using access control matrix*. Proceedings of the 3rd International Conference on Computing, Communications Technology and Networking, July 21-25, 2012, Tamilnadu, India, pp.750-765.

Monfared, A.T., & Jaatun, M.G. (2011). *Monitoring intrusions and security breaches in highly distributed cloud environments,* IEEE 3rd international conference on cloud computing technology and science. Athens, Greece, pp 772–777.

Munoz, A., Gonzalez, J., & Mana, A. (2012, August). A Performance-Oriented Monitoring System for Security Properties in Cloud Computing Applications. Computer Journal, 55(8), 979-994.

Nishikawa, K., Oki, K., & Matsuo A. (2012, December 4-7). *SaaS application framework using information gateway enabling cloud service with data confidentiality. Software Engineering Conference* (APSEC), 2012 19th Asia-Pacific, pp. 334-337. Hong Kong, China.

Ranger, S (2017, November 15). *The future of cyberwar: Weaponized ransomware, IoT attacks, and a new arms race*. TechRepublic. https://www.techrepublic.com/article/the-future-of-cyberwar-weaponised-ransomware-iot-attacks-and-a-new-arms-race/.

Ryan, P., & Watson, R. (2017). Research Challenges for the Internet of Things: What Role Can OR Play? *Systems*, 5(24), 2-32.

Strauss & Corbin (2015). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*, 2nd Edition. Sage Publications. Thousand Oaks, CA.

Von Bertalanffy, L. (1968). General Systems Theory: Foundations, Development, Applications. *JAMA*, 208, 870.

Wang, J., Liao, J., Li, T., & Wang, J. (2016). Game –theoretic model of asymmetrical multipath selection in pervavis computing environment. *Pervasive Mobile Computing*, 27, 37-57.

Yao, B., Liu, X., Zhang, W., Chen, X., Yao, M. & Zhao, Z. (2013, Noevember 13-15). *Applying Graph Theory to the Internet of Things.* Proceedings of the 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, Zhangjiajie, China.

Yin, R. (1994). *Case Study Research: Design and Methods.* Sage Publications. Thousand Oaks, CA.

Zhu, J., & Wen, Q. (2012, November 23-25). *SaaS access control research based on UCON*. Digital Home (ICDH), 2012 Fourth International Conference. Guangzhou, China, pp.331.