Understanding Taxonomy of Cyber Risks for Cybersecurity Insurance of Financial Industry in Cloud Computing

Sam Adam Elnagdy[1], Meikang Qiu[2*], Keke Gai[3]

***Abstract*—The dramatical development of Web-based technology has been empowering enormous change in various domains. Cloud-based solutions have remarkably widened business models with multiple value creation channels. The financial industry is a major beneficiary of leveraging these emerging new technologies, such as big data and cloud-related services. This great changing trend has also led to a great concern in cybersecurity. Under this background, cybersecurity insurance is a growing domain in the financial industry. However, cybersecurity insurance industry also encounters a variety of cyber concerns while the Web-based approaches are applied. This paper focuses on this issue and review a broad scope of materials to gain a deep understanding of taxonomy of cyber security risks for cybersecurity insurance. The findings of this work can guide the cybersecurity insurance practitioners to avoid as much risk as possible as well as create potential solutions to the possible risks.**

***Index Terms*—Cyber security, risk taxonomy, cybersecurity insurance, financial industry, cloud computing**

I. Introduction

Contemporarily, cybersecurity risks have been considered a significant issue in multiple fields. Considering a higher-level security requirement, the financial industry also has a critical concern when *Financial Service Institutions* (FSIs) is applying networking-based solutions [1]–[3]. A remarkable growing demand of storing sensitive data in digital forms has enabled many implementations of new technologies, such as cloud computing [4], big data [5], and *Internet-of-Things* (IoT). This development trend has led to distributed storage and a broad utilization of virtual machines [6]. Without the geographical limitations, data can be transmitted, shared, stored, and operated over the wired or wireless network systems. This ongoing change not only empowers financial firms' capability in value creations but also brings a variety of challenges to financial practitioners and enterprises [7].

[1] S. Elnagdy is with Department of Computer Science, Pace University, New York, NY, 10038, se85420n@pace.edu;

[2] M. Qiu is with Department of Computer Science, Pace University, New York, NY 10038, USA, mqiu@pace.edu;

[3] K. Gai is with Department of Computer Science, Pace University, New York, NY 10038, USA, kg71231w@pace.edu;

* M. Qiu is the corresponding author of this paper. Email address: mqiu@pace.edu.

** This work is supported by NSF CNS-1457506 and NSF CNS-1359557. (Prof. M. Qiu).

There are numerous existing cyber risks threatening FSIs that are using networking-related solutions [8]. The fundamental of avoiding and solving these threats is to be aware of those cyber risks [9]. However, understanding cyber risks taxonomy is a challenging task due to the high complexity of the entity-entity relations and the broad crossed disciplines. This paper addresses this issue and accomplishes a survey that focuses on the cybersecurity issues related to cybersecurity insurance in the financial industry.

The significance of our research work is solid and straightforward. Most current implemented cybersecurity insurance solutions are struggling with a few obstructions, such as immature information sharing mechanism, undeveloped cyber incident analytics, and lack of effective risk management for cybersecurity [10]. These issues can result in arguable definitions of itemizing cybersecurity insurance coverages or lead to ambiguous representations of cyber incidents' contexts. Therefore, a common solution to contemporary cybersecurity insurance in the financial industry is simply cover most aspects in cybersecurity, which also simply causes remarkable high costs. For achieving lower costs, a granular awareness of the cyber risk facts in the financial industry is required and urgent. Therefore, our research work is important for both researchers and practitioners in the domain of cybersecurity insurance.

Fig. 1 represents a mapping structure of our survey work. Three vital aspects of cybersecurity insurance are covered in our work, namely risk management, taxonomy, and techniques. A few sub-objects are involved in each aspect. This paper follows the structure shown in Fig. 1 to concisely represent the knowledge structure at the target field.

In addition, the main contributions of this paper are:

1) We build up a knowledge structure of cybersecurity insurance in order to assist practitioners to obtain a granular cognition of the knowledge. A deep awareness of cybersecurity insurance will provide a potential of reducing the insurance cost.
2) The findings and discussions in this paper provide researchers with references and a guideline of future research work.

978-1-5090-0946-6/16 $31.00 © 2016 IEEE
DOI 10.1109/CSCloud.2016.46

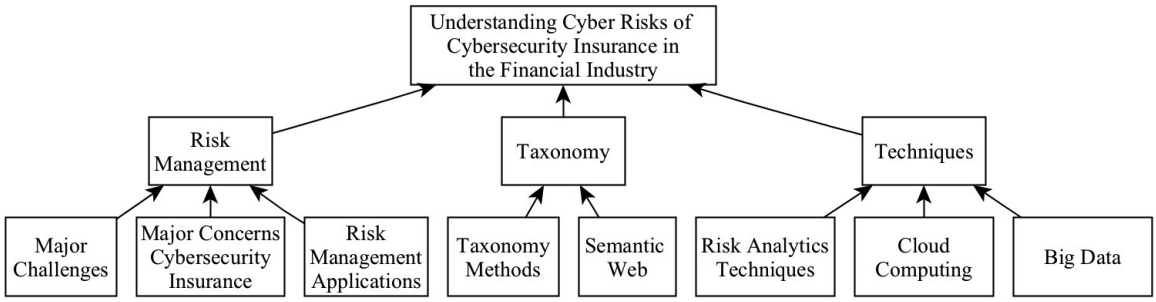

Fig. 1: Mapping structure of the survey work

We organize the rest of this paper by structurializing the knowledge structure concerning the cybersecurity insurance. Section II reviews crucial risk management methods in cybersecurity insurance. Next, Section III converges main techniques contemporarily used in cybersecurity insurance. Furthermore, we summarize and categorize cyber incidents taxonomy of cybersecurity insurance in Section IV. Finally, we provide the conclusions in Section V.

II. Risk Management in Cybersecurity Insurance

A. Risk Management Applications

Risk management is a significant component of ensuring financial safe, which is also an important aspect of cybersecurity insurance [11]. The implementations of financial risk management have played a critical role in securing financial operations, because the risk management methods will determine the practical effects from risk predictions to solution designs. The target risk management model needs to be validated by financial analysts and data experts in order to ensure the flexibility and correctness of the applied model [12]–[14].

Moreover, with the development of the Internet technologies, the coverage of the risk management is also attached to the cyber threats analyses and model validations [15]. Focusing on current financial firms, many cyber risks are categorized into three layers, including strategical, tactical, and operational layers [16], [17]. Each layer requires specific demands, management method, and designed solutions. For the purpose of protecting information, for instance, there are mainly three aspects that are needed to be considered, which include confidentiality, integrity, and availability [18].

Furthermore, there are many techniques currently being applied in financial risk management domains. For instance, establishing a secure business operation system is an efficient option for most financial companies to increase the security level without adding much hardware facilities [19], [20]. Most contemporary popular analysis approaches derive from statistics, which concentrate on the structured data [21], [22]. This situation is switching to a broader application scope due to the emergence of big data techniques. Semi-structured and unstructured data have been brought into the financial cyber risk models in recent researches [23], [24]. The higher-level data complexity required the optimizations of big data [25].

B. Major Concerns of Cybersecurity Insurance

According to the Homeland Security Department's report, there are a number of major concerns in current cybersecurity insurance [26]. These concerns can hardly build up a healthy relationship with the coverage satisfaction.

First, establishing a comprehensive cybersecurity insurance system is challenging because rare terms can be derived from the existing commercial insurance policies. This phenomenon results in a few negative effects, such as a wide robust coverage and ambiguous obligation statements. Second, applying current cybersecurity insurance will bring a heavy financial burden to FSIs due to the non-classified insurance policies with a broad coverage scope. Most cybersecurity insurance policies try to cover a larger sized cyber incidents in order to avoid the confusing obligations. Finally, hardware infrastructure's physical damages may provide adversaries with attack opportunities; however, this growing risks are rarely addressed by current cybersecurity insurance policies due to the complexity of identifying the causality of the cyber incidents.

Moreover, Pal et al. [27] accomplished an investigation in the effects of cybersecurity insurance from the marketing reaction perspective. According to this work, the authors addressed two market types, namely monopolistic and competitive cybersecurity insurance markets. Based on a broad data gathering, there were two findings of this research. First, there was no sufficient diversity between two market types when the contract discriminations among insurance clients were not applied, even though it seemed that an equilibrium point existed. Second, applying contract discrimination in monopoly markets could improve network security. This research implied that markets had limited impacts on reducing concerns of cybersecurity insurance.

C. Major Challenges

Identifying the obligations is a complicated issue in which a large volume of interconnections and interrelations exist between entities. The cause effect relationships between cyber incidents and cyber risks are hard to be accurately defined, because there are rarely one-to-one relations. Most situations represent a multi-to-multi relation. This is also one of the reasons why current cybersecurity insurance policies mainly offer broad service scopes.

Moreover, an ambiguous representation of cybersecurity entities can also cause confusions when direction and indirect relations synchronously exist. Sometimes, a chain reaction occurs such that the cause effect relations are difficult to be identified from the intercrossed complex entity networks. The cause of the chain reactions could be the data destruction, hacking attacks, *Denial of Service* (DoS), and illegal adversaries [28].

Furthermore, the boundary between hardware and software is not so clear in cybersecurity insurance domain [29], [30]. The reason why the challenge exists is because any part's damage may weaken the other part. For example, physical infrastructure damages will increase the chance of being attacked by adversaries at data transmission layer or database layer. The indirect relations between infrastructures or applications can produce unanticipated vulnerabilities. In a cloud system, a serious data bleach can be created if adversaries can successfully map the cloud infrastructure.

Next, some previous researches proved that one of the vital challenges of cybersecurity is human-related operating errors [31]. The argument of this perspective stated that many system threats took place when end users open some phishing document by accident or have improper operations without effective protection mechanism.

III. Main Techniques in Cybersecurity Insurance

We focus on three popular techniques that are forming the mainstream of cybersecurity insurance in this section. Three techniques include big data, cloud computing, and data analytic techniques.

A. Big Data in Cybersecurity Insurance

The technology of big data is an emerging term that represents the techniques gaining valuable information from large volume of data [32]–[34]. The implementations of big data can be found in a large scope of fields, which have been also addressed by recent researches [35]. For example, using big data techniques can efficiently avoid fraud or counterfeit information over the e-commerce platform [36]. The analysis results of big data can be used as a reference for detecting improper commerical behaviors. In addition, Monte Carlo simulation is often considered an effective method of obtaining results from a dramatical large sized dataset [37].

Moreover, improving efficiency of big data analysis has been explored by recent researches as well [38]. For example, a classification algorithm was proposed to increase the classification performance using ensemble feature selections for imbalanced-class dataset [39]. In the financial industry, meta-analytics methods were proved as an effective method for forecasting risks when meta-regression was applied [40]. Another research focusing on optimizing computing efficiency proposed a scheme using pre-cache techniques to achieve high performance of telehealth systems [41].

In addition, one major characteristic of current cybersecurity insurance is that most analyses mainly address the structured data. Many data mining techniques can simply dig information from a pool of structured data that derive from different data sources [42], [43]. This is also a major concern in the privacy protection domain. For instance, financial customers' accounts consist of abundant sensitive information. Sometimes, FSIs need to share some data with the third party for the purpose of data analysis. In order to protect financial customers' privacy, FSIs usually provide only partial dataset rather than the whole dataset. This approach is facing a great challenge due to the broad implementations of data mining in big data. Sensitive information can be gained when the third parts use data mining and data integration techniques. The privacy leakage can take place when the third party combines various data components from the same data source.

B. Cloud Computing Implementations

Cloud computing is another emerging technical term that provides a flexible remote computing resource sharing method. *Platform-as-a-Service* (PaaS) is one of popular service models that has been broadly accepted by many service offering organizations [44], [45]. The performance enhancement has been paid sufficient attentions in various perspectives [46], [47]. Many algorithms have been proposed in order to increase cloud systems' performance, such as genetic algorithm [48], [49], dynamic programming [50]–[52], and Greedy algorithm [53], [54].

Considering privacy and security issues, many previous researches had explored higher-level cloud-based protections for financial firms [43], [55]. For example, recent research has proved that using attribute-based semantic access controls could proactively secure data owners' data in mobile cloud computing [56]. In this method, data attributes are emphasized and it aimed to avoid cyber risks by identifying data users' statuses. Similarly, multimedia big data in cloud computing could also secured by identifying the data users' behaviors and standings [57].

Moreover, Gai et al. [58] converge most recent intrusion detection techniques for mobile cloud computing in

heterogeneous 5G. The findings of this search also include summarizing intrusion types in wireless networks. Another survey was done by Thakur et al. [59] who focused on cyber threats and security models. These prior investigations provide theoretical fundamental for categorizing cyber threats.

C. Risk Analytics Techniques in Cybersecurity Insurance

Risk analytics techniques have been dramatically improved in recent years. Most current analytics techniques derive from a few classic analytic tools, such as *Bayesian Tree*, *Associated Rules*, and *Regression*. For example, security risk management could use dynamic bayesian attack graphs to reduce the impact of adversaries [60].

Moreover, the emerging mainstream of big data is shifting many domains from analytics-oriented to intelligent-oriented approaches. For example, Zeng and Lusch [61] argued that future business approaches would swift from transaction-based to ecosystems-based models. They emphasizes the information gains from the systemic-based data pools by which the rich knowledge pools are generated. Similar insights were also addressed by other scholars who attempted to explore the efficient information acquisitions [62], [63]. New terms have been created for describing this new trend, such as data-centric or data-intensive approach [64].

IV. Cyber Incidents Taxonomy in Cybersecurity Insurance

A. Taxonomy Methods

Taxonomy is an effective approach for organizing the knowledge body by classifying entities. In the field of cybersecurity insurance, the vital issue is finding out the methods of creating taxonomy of cybersecurity, which is the fundamental of organizing cyber incidents and relevant technical issues in a group-based manner. Many prior researches have proved that using taxonomy-based approaches can categorize objects for reaching certain purposes [65], [66]. The method of the taxonomy usually depends on the perspective defining the variety.

Next, many perspectives have been addressed by the prior researches in cybersecurity. One approach is to categorize security issues into two main perspectives, including interior and exterior perspectives [67]. For instance, cyber attackers can be grouped into two categories, which are insider and outsider attackers. This method is often used for analyzing risks related to user attributes and infrastructure utilizations.

Another method of taxonomy is to use attributes or features to diversify objects. This method usually applies the data mining techniques to extract the characteristics of data, entities, or objects. For example, analyzing correlations among a group of interrelated objects is an approach for classifying the target, such as networking traffics [68] and e-commercial performance [69]. This goal can be achieved by using a variety of machine learning techniques, such as Naive Bayes predictions [70] or decision trees.

Moreover, knowledge graph is an approach representing the relations between entities in the system, which has been paid a high attention by researchers recently. Combing knowledge graph with ontology is an efficient approach for representing knowledge and managing information [71]. One major advantage of using ontology-based solution with combing knowledge graphs is that relations between entities can be defined by using updated languages, such as *Web Ontology Language* (OWL). Utilizing this advantage is considered an effective alternative for identifying the complicated direct or indirect relations between entities [72], [73]. Performances can be also improved while other techniques are integrated, such as cloud computing [74].

B. Semantic Web

Semantic web is an efficient Web platform supporting ontology-based solutions [75]. Many prior researches explored the implementations in practice, from telehealth [76] to financial services [56]. Recent researches also addressed the integrated syntax and semantic validations for service computing [77]. Many researches have proved that using semantic Web techniques can enable to build up quality service models with linked services within a network environment [78], [79]. Integrating Web services with other computing resources can empower the whole computing system and provision flexible service delivery methods [80]. Moreover, ontology-based solutions are often integrated with semantic Web to solve the security and privacy issues. Therefore, using semantic Web and ontology-based knowledge representation can be approach of identifying the complex direct and indirect relations in cybersecurity insurance, which is a vital component of understanding cybersecurity insurance's risks and concerns.

V. Conclusions and Future Work

This paper represented a survey in taxonomy of cybersecurity risks in the domain of cybersecurity insurance. The literature review covered three crucial aspects of cybersecurity insurance, including risk management, main active techniques, and cyber incidents. An empirical study was shown in this work as well. Our findings could be used as a reference for further research in cybersecurity insurance.

References

[1] K. Gai, M. Qiu, and S. Elnagdy. Security-aware information classifications using supervised learning for cloud-based cyber risk management in financial big data. In *The 2nd IEEE International Conference on Big Data Security on Cloud*, pages 197–202, New York, USA, 2016.

[2] K. Gai and A. Steenkamp. Feasibility of a platform-as-a-service implementation using cloud computing for a global service organization. In *Proceedings of the Conference for Information Systems Applied Research*, volume 2167, pages 1508–1523, 2013.

[3] K. Gai. A review of leveraging private cloud computing in financial service institutions: Value propositions and current performances. *Int'l J. of Computer Applications*, 95(3):40–44, 2014.

[4] K. Gai and S. Li. Towards cloud computing: a literature review on cloud computing and its development trends. In *2012 Fourth Int'l Conf. on Multimedia Information Networking and Security*, pages 142–146, Nanjing, China, 2012.

[5] H. Yin and K. Gai. An empirical study on preprocessing high-dimensional class-imbalanced data for classification. In *The IEEE International Symposium on Big Data Security on Cloud*, pages 1314–1319, New York, USA, 2015.

[6] K. Gai, M. Qiu, and H. Zhao. Security-aware efficient mass distributed storage approach for cloud systems in big data. In *The 2nd IEEE International Conference on Big Data Security on Cloud*, pages 140–145, New York, USA, 2016.

[7] A. Steenkamp, A. Alawdah, O. Almasri, K. Gai, N. Khattab, C. Swaby, and R. Abaas. Teaching case enterprise architecture specification case study. *Journal of Information Systems Education*, 24(2):105, 2013.

[8] K. Gai, M. Qiu, B. Thuraisingham, and L. Tao. Proactive attribute-based secure data schema for mobile cloud in financial industry. In *The IEEE International Symposium on Big Data Security on Cloud; 17th IEEE International Conference on High Performance Computing and Communications*, pages 1332–1337, New York, USA, 2015.

[9] K. Gai, M. Qiu, and S. Elnagdy. A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance. In *The 2nd IEEE International Conference on Big Data Security on Cloud*, pages 171–176, New York, USA, 2016.

[10] H. Jean-Baptiste, L. Tao, M. Qiu, and K. Gai. Model risk management systems-back-end, middleware, front-end and analytics. In *The 2nd IEEE International Conference on Cyber Security and Cloud Computing*, pages 312–316, New York, USA, 2015. IEEE.

[11] F. Caron, J. Vanthienen, and B. Baesens. A comprehensive investigation of the applicability of process mining techniques for enterprise risk management. *Computers in Industry*, 64(4):464–475, 2013.

[12] M. Uzzafer. A contingency estimation model for software projects. *International Journal of Project Management*, 31(7):981–993, 2013.

[13] K. Gai and J. Pan. Human resource management: A case study of the air traffic controller strike in 1981. *China Management Informationization*, 12(15):61–65, 2015.

[14] G. Dionne. Risk management: history, definition, and critique. *Risk Management and Insurance Review*, 16(2):147–166, 2013.

[15] H. Jean-Baptiste, L. Tao, K. Gai, and M. Qiu. Understanding model risk management - model rationalization in financial industry. In *The 2nd IEEE International Conference on Cyber Security and Cloud Computing*, pages 301–306, New York, USA, 2015. IEEE.

[16] Y. Malhotra. Cybersecurity & cyber-finance risk management: Strategies, tactics, operations, &, intelligence: Enterprise risk management to model risk management: Understanding vulnerabilities, threats, & risk mitigation. *Tactics, Operations, &, Intelligence: Enterprise Risk Management to Model Risk Management: Understanding Vulnerabilities, Threats, & Risk Mitigation (September 15, 2015)*, 2015.

[17] S. Amin, G. Schwartz, and A. Hussain. In quest of benchmarking security risks to cyber-physical systems. *IEEE Network*, 27(1):19–24, 2013.

[18] J. Webb, A. Ahmad, S. Maynard, and G. Shanks. A situation awareness model for information security risk management. *Computers & security*, 44:1–15, 2014.

[19] O. Lavastre, A. Gunasekaran, and A. Spalanzani. Supply chain risk management in french companies. *Decision Support Systems*, 52(4):828–838, 2012.

[20] Y. Yang, H. Shieh, and G. Tzeng. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. *Information Sciences*, 232:482–500, 2013.

[21] E. Brechmann and C. Czado. Risk management with high-dimensional vine copulas: An analysis of the Euro Stoxx 50. *Statistics & Risk Modeling*, 30(4):307–342, 2013.

[22] S. Hammoudeh, P. Santos, and A. Al-Hassan. Downside risk management and var-based optimal portfolios for precious metals, oil and stocks. *The North American Journal of Economics and Finance*, 25:318–334, 2013.

[23] D. O'Leary. Artificial intelligence and big data. *IEEE Intelligent Systems*, 28(2):96–99, 2013.

[24] H. Hu, Y. Wen, T. Chua, and X. Li. Toward scalable systems for big data analytics: a technology tutorial. *IEEE Access*, 2:652–687, 2014.

[25] J. Wang, M. Qiu, B. Guo, and Z. Zong. Phase-reconfigurable shuffle optimization for Hadoop MapReduce. *IEEE Transactions on Cloud Computing*, PP(99):1, 2015.

[26] DHS. Cybersecurity insurance, 2015. Retrieve from Forbes.com at http://www.dhs.gov/cybersecurity-insurance.

[27] R. Pal, L. Golubchik, K. Psounis, and P. Hui. Will cyber-insurance improve network security? a market analysis. In *Proceedings IEEE INFOCOM*, pages 235–243, Toronto, ON, Canada, 2014. IEEE.

[28] L. Ma, L. Tao, Y. Zhong, and K. Gai. RuleSN: Research and application of social network access control model. In *IEEE International Conference on Intelligent Data and Security*, pages 418–423, New York, USA, 2016.

[29] B. Boyd. Cloud control: managing the risks of engaging and terminating cloud services. *Information Management Journal*, 48(6):20–26, 2014.

[30] S. Donaldson, S. Siegel, C. Williams, and A. Aslam. Meeting the cybersecurity challenge. In *Enterprise Cybersecurity*, pages 27–44. Springer, 2015.

[31] D. Norris, A. Joshi, and T. Finin. Cybersecurity challenges to american state and local governments. In *15th European Conference on eGovernment*, pages 196–202. Academic Conferences and Publishing Int. Ltd., 2015.

[32] H. Chen, R. Chiang, and V. Storey. Business intelligence and analytics: From big data to big impact. *MIS quarterly*, 36(4):1165–1188, 2012.

[33] X. Yu, T. Pei, K. Gai, and L. Guo. Analysis on urban collective call behavior to earthquake. In *The IEEE International Symposium on Big Data Security on Cloud*, pages 1302–1307, New York, USA, 2015. IEEE.

[34] X. He, C. Wang, T. Liu, K. Gai, D. Chen, and L. Bai. Research on campus mobile model based on periodic purpose for opportunistic network. In *2015 IEEE 17th International Conference on High Performance Computing and Communications*, pages 782–785, New York, USA, 2015. IEEE.

[35] K. Gai, M. Qiu, L. Chen, and M. Liu. Electronic health record error prevention approach using ontology in big data. In *17th IEEE International Conference on High Performance Computing and Communications*, pages 752–757, New York, USA, 2015.

[36] H. Liang and K. Gai. Internet-based anti-counterfeiting pattern with using big data in china. In *The IEEE International Symposium on Big Data Security on Cloud*, pages 1387–1392, New York, USA, 2015. IEEE.

[37] M. Qiu, D. Cao, H. Su, and K. Gai. Data transfer minimization for financial derivative pricing using Monte Carlo simulation with GPU in 5G. *International Journal of Communication Systems*, 2015.

[38] S. Ding, X. He, J. Wang, B. Qiao, and K. Gai. Static node center opportunistic coverage and hexagonal deployment in hybrid crowd sensing. *Journal of Signal Processing Systems*, pages 1–17, 2016.

[39] H. Yin, K. Gai, and Z. Wang. A classification algorithm based on ensemble feature selections for imbalanced-class dataset. In *The 2nd IEEE International Conference on High Performance and Smart Computing*, pages 245–249, New York, USA, 2016.

[40] H. Jean-Baptiste, M. Qiu, K. Gai, and L. Tao. Meta meta-analytics for risk forecast using big data meta-regression in financial industry. In *The 2nd IEEE International Conference on Cyber Security and Cloud Computing*, pages 272–277, New York, USA, 2015. IEEE.

[41] H. Zhao, K. Gai, J. Li, and X. He. Novel differential schema for high performance big data telehealth systems using pre-cache. In *The IEEE International Symposium on Big Data Security on Cloud, IEEE 17th International Conference on High Performance Computing and Communications*, pages 1412–1417. IEEE, 2015.

[42] J. Servidio and R. Taylor. Safe and sound: Cybersecurity for community banks. *Journal of Taxation & Regulation of Financial Institutions*, 28(4), 2015.

[43] Y. Li, W. Dai, Z. Ming, and M. Qiu. Privacy protection for preventing data over-collection in smart city. *IEEE Transactions on Computers*, PP:1, 2015.

[44] K. Gai and A. Steenkamp. A feasibility study of Platform-as-a-Service using cloud computing for a global service organization. *Journal of Information System Applied Research*, 7:28–42, 2014.

[45] H. Zhao, M. Chen, M. Qiu, K. Gai, and M. Liu. A novel pre-cache schema for high performance Android system. *Future Generation Computer Systems*, 2015.

[46] K. Gai, M. Qiu, H. Zhao, L. Tao, and Z. Zong. Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. *Journal of Network and Computer Applications*, 59:46–54, 2015.

[47] K. Gai, Z. Du, M. Qiu, and H. Zhao. Efficiency-aware workload optimizations of heterogenous cloud computing for capacity planning in financial industry. In *The 2nd IEEE International Conference on Cyber Security and Cloud Computing*, pages 1–6, New York, USA, 2015. IEEE.

[48] M. Qiu, M. Zhong, J. Li, K. Gai, and Z. Zong. Phase-change memory optimization for green cloud with genetic algorithm. *IEEE Transactions on Computers*, 64(12):3528 – 3540, 2015.

[49] M. Qiu, Z. Chen, J. Niu, G. Quan, X. Qin, and L. Yang. Data allocation for hybrid memory with genetic algorithm. *IEEE Transactions on Emerging Topics in Computing*, pp:1–11, 2015.

[50] J. Li, M. Qiu, J. Niu, L. Yang, Y. Zhu, and Z. Ming. Thermal-aware task scheduling in 3D chip multiprocessor with real-time constrained workloads. *ACM Transactions on Embedded Computing Systems*, 12(2):24, 2013.

[51] M. Qiu and E. Sha. Cost minimization while satisfying hard/soft timing constraints for heterogeneous embedded systems. *ACM Trans. on Design Automation of Electronic Syst.*, 14(2):25, 2009.

[52] M. Qiu, Z. Chen, Z. Ming, X. Qin, and J. Niu. Energy-aware data allocation with hybrid memory for mobile cloud systems. *IEEE Systems Journal*, PP:1–10, 2014.

[53] J. Li, M. Qiu, Z. Ming, G. Quan, X. Qin, and Z. Gu. Online optimization for scheduling preemptable tasks on IaaS cloud systems. *Journal of Parallel and Distributed Computing*, 72(5):666–677, 2012.

[54] L. Chen, Y. Duan, M. Qiu, J. Xiong, and K. Gai. Adaptive resource allocation optimization in heterogeneous mobile cloud systems. In *The 2nd IEEE International Conference on Cyber Security and Cloud Computing*, pages 19–24, New York, USA, 2015. IEEE.

[55] M. Qiu, W. Gao, M. Chen, J. Niu, and L. Zhang. Energy efficient security algorithm for power grid wide area monitoring system. *IEEE Transactions on Smart Grid*, 2(4):715–723, 2011.

[56] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, and H. Zhao. Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. *Future Generation Computer Systems*, PP:1, 2016.

[57] Y. Li, K. Gai, Z. Ming, H. Zhao, and M. Qiu. Intercrossed access control for secure financial services on multimedia big data in cloud systems. *ACM Transactions on Multimedia Computing Communications and Applications*, PP(99):1, 2016.

[58] K. Gai, M. Qiu, L. Tao, and Y. Zhu. Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. *Security and Communication Networks*, pages 1–10, 2015.

[59] K. Thakur, M. Qiu, K. Gai., and M. Ali. An investigation on cyber security threats and security models. In *The 2nd IEEE International Conference on Cyber Security and Cloud Computing*, pages 307–311, New York, USA, 2015. IEEE.

[60] N. Poolsappasit, R. Dewri, and I. Ray. Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 9(1):61–74, 2012.

[61] D. Zeng and R. Lusch. Big data analytics: Perspective shifting from transactions to ecosystems. *IEEE Intelligent Systems*, 28(2):2–5, 2013.

[62] G. Wu, H. Zhang, M. Qiu, Z. Ming, J. Li, and X. Qin. A decentralized approach for mining event correlations in distributed system monitoring. *Journal of parallel and Distributed Computing*, 73(3):330–340, 2013.

[63] M. Qiu, Z. Ming, J. Li, , S. Liu, B. Wang, and Z. Lu. Three-phase time-aware energy minimization with DVFS and unrolling for chip multiprocessors. *J. of Syst. Architecture*, 58(10):439–445, 2012.

[64] C. Chen and C. Zhang. Data-intensive applications, challenges, techniques and technologies: A survey on big data. *Information Sciences*, 275:314–347, 2014.

[65] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu. Securing smart grid: cyber attacks, countermeasures, and challenges. *IEEE Communications Magazine*, 50(8):38–45, 2012.

[66] Q. Jing, A. Vasilakos, J. Wan, J. Lu, and D. Qiu. Security of the internet of things: Perspectives and challenges. *Wireless Networks*, 20(8):2481–2501, 2014.

[67] E. Bompard, T. Huang, Y. Wu, and M. Cremenescu. Classification and trend analysis of threats origins to the security of power systems. *International Journal of Electrical Power & Energy Systems*, 50:50–64, 2013.

[68] J. Zhang, Y. Xiang, Y. Wang, W. Zhou, Y. Xiang, and Y. Guan. Network traffic classification using correlation information. *IEEE Transactions on Parallel and Distributed Systems*, 24(1):104–117, 2013.

[69] K. Gai, M. Qiu, H. Zhao, and W. Dai. Anti-counterfeit schema using monte carlo simulation for e-commerce in cloud systems. In *The 2nd IEEE International Conference on Cyber Security and Cloud Computing*, pages 74–79, New York, USA, 2015. IEEE.

[70] J. Zhang, C. Chen, Y. Xiang, W. Zhou, and Y. Xiang. Internet traffic classification by aggregating correlated naive bayes predictions. *IEEE Transactions on Information Forensics and Security*, 8(1):5–15, 2013.

[71] J. Liu, Y. He, E. Lim, and X. Wang. A new method for knowledge and information management domain ontology graph model. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 43(1):115–127, 2013.

[72] Z. Xu, H. Zhang, C. Hu, L. Mei, J. Xuan, and et. al. Building knowledge base of urban emergency events based on crowdsourcing of social media. *Concurrency and Computation: Practice and Experience*, 2016.

[73] A. De Nicola and M. Missikoff. A lightweight methodology for rapid ontology engineering. *Communications of the ACM*, 59(3):79–86, 2016.

[74] V. Stantchev, L. Prieto-González, and G. Tamm. Cloud computing service for knowledge assessment and studies recommendation in crowdsourcing and collaborative learning environments based on social network analysis. *Computers in Human Behavior*, 51:762–770, 2015.

[75] S. Gollapudi. Aggregating financial services data without assumptions: A semantic data reference architecture. In *IEEE Int'l Conf. on Semantic Computing*, pages 312–315, Anaheim, CA, USA, 2015.

[76] K. Gai, M. Qiu, S. Jayaraman, and L. Tao. Ontology-based knowledge representation for secure self-diagnosis in patient-centered telehealth with cloud systems. In *The 2nd IEEE International Conference on Cyber Security and Cloud Computing*, pages 98–103, New York, USA, 2015. IEEE.

[77] L. Tao, S. Golikov, K. Gai, and M. Qiu. A reusable software component for integrated syntax and semantic validation for services computing. In *9th Int'l IEEE Symposium on Service-Oriented System Engineering*, pages 127–132, San Francisco Bay, USA, 2015.

[78] W. Chen, I. Paik, and P. Hung. Constructing a global social service network for better quality of web service discovery. *IEEE Transactions on Services Computing*, 8(2):284–298, 2015.

[79] I. Farris, R. Girau, M. Nitti, L. Atzori, R. Bruschi, A. Iera, and G. Morabito. Taking the SIoT down from the cloud: Integrating the social internet of things in the INPUT architecture. In *IEEE 2nd World Forum on Internet of Things*, pages 35–39, Milan, Italy, 2015. IEEE.

[80] P. Melliar-Smith and L. Moser. Conversion infrastructure for maintaining high availability of web services using multiple service providers. In *IEEE International Conference on Web Services*, pages 759–764, New York, NY, USA, 2015. IEEE.