Protecting Critical Cloud Infrastructures with Predictive Capability

Stephen S. Yau, Arun Balaji Buduru and Vinjith Nagaraja
Information Assurance Center, and
School of Computing, Informatics, and Decision Systems Engineering
Arizona State University, Tempe, AZ, USA
{yau, abuduru and vnagar10}@asu.edu

Abstract: **Emerging trends in cyber system security breaches, including those in critical infrastructures involving cloud systems, such as in applications of military, homeland security, finance, utilities and transportation systems, have shown that attackers have abundant resources, including both human and computing power, to launch attacks. The sophistication and resources used in attacks reflect that the attackers may be supported by large organizations and in some cases by foreign governments. Hence, there is an urgent need to develop intelligent cyber defense approaches to better protecting critical cloud infrastructures. In order to have much better protection for critical cloud infrastructures, effective approaches with predictive capability are needed. Much research has been done by applying game theory to generating adversarial models for predictive defense of critical infrastructures. However, these approaches have serious limitations, some of which are due to the assumptions used in these approaches, such as rationality and Nash equilibrium, which may not be valid for current and emerging cloud infrastructures. Another major limitation of these approaches is that they do not capture probabilistic human behaviors accurately, and hence do not incorporate human behaviors. In order to greatly improve the protection of critical cloud infrastructures, it is necessary to predict potential security breaches on critical cloud infrastructures with accurate system-wide causal relationship and probabilistic human behaviors. In this paper, the challenges and our vision on developing such proactive protection approaches are discussed.**

Keywords: *Critical cloud infrastructures, security breaches, pro-active protection, predictive defense, probabilistic reasoning, and probabilistic human behaviors*

I. INTRODUCTION

Emerging trends in cyber system security breaches, including those in critical infrastructures, which increasingly use cloud infrastructures, such as in military, homeland security, finance, utilities and transportation systems have shown that attackers are no longer limited by resources, including human and computing power. The sophistication and resources used in attacks reflect that they may be supported by large organizations and in some cases by foreign governments [1]. Hence, there is an urgent need to develop proactive defense approaches to protecting critical cloud infrastructures. In this paper, we will discuss the challenges and possible solutions for developing such an approach to proactively protecting critical cloud infrastructures.

This paper is organized as follows: In Section II, we will discuss our vision on the challenges of providing proactive defense for critical cloud infrastructures, and how to improve such protection. In Section III, we will discuss the existing approaches to protecting critical cloud infrastructures, and their limitations. In Section IV, we will present our vision on developing a proactive defense approach with predictive capability for better protection of critical cloud infrastructures. In Section V, we will provide an illustration for this approach. In Section VI, we will discuss some research issues which need to be addressed in order to make such an approach reality.

II. CHALLENGES AND IMPROVEMENTS

In cloud infrastructures, there are many security challenges, including insider threats, outsider malicious attacks, data loss, issues related to multi-tenancy, cryptographic key ownership, loss of control and service disruption [2]. For critical cloud infrastructures, due to the very serious impacts of their security breaches, besides the above security challenges, we also need to address the following major challenges:

C1) User-centric Security Systems: The usability of security systems is one of the primary factors determining the effectiveness of the security systems. Most security systems do not sufficiently incorporate usability factors, such as users' preferences and behaviors. Incorporating users' preferences and behaviors, and including certain degree of prediction of human behaviors are needed for developing user-centric security systems for critical cloud infrastructures. This is a major challenge for providing better protection of critical cloud infrastructures because human behaviors are intrinsically probabilistic in nature and require a probabilistic framework for capturing and analyzing human preferences and behaviors

C2) Emergence of Software Defined Network (SDN): Increasingly, many large-scale cloud infrastructures are using SDN architectures to improve their operational efficiencies. The most significant advantage of SDN is to provide efficient network agility and management through a centralized control of network architecture. From security point of view, the centralized control structure is also its most serious disadvantage because moving the network from relatively decentralized structure to centralized controller environment will significantly

2159-6190/15 $31.00 © 2015 IEEE
DOI 10.1109/CLOUD.2015.165

increase the risk of potential single point of attack and causing catastrophic failure.

C3) Low Overhead for Security Measures to Maintain High Operational Efficiency: In order to be profitable, the high efficiency and fast turnaround of various tasks of critical cloud infrastructures are required. Hence, the security measures for critical cloud infrastructures must introduce little overhead since currently they are run all the time when the critical cloud infrastructures are in service.

To address these challenges, we need to have effective approaches with predictive capability to enable the critical cloud infrastructures to prevent security breaches. In order to have such approaches with predictive capability, accurate threat assessment and operational behavioral modelling of the critical cloud infrastructures are required. Since probabilistic human behaviors affect the system operational behavior, it is imperative that such approaches should have some frameworks to facilitate the capturing and analyses of probabilistic human behaviors accurately and efficiently. Several organizations have already considered such approaches [2, 3].

III. CURRENT STATE OF THE ART

Existing approaches to protecting cyber infrastructures with predictive capability are based on applying game theory to generating adversarial models [4-12]. However, these approaches have certain serious limitations. Some of these approaches [4-7] have the limitations due to the assumptions used, such as the rationality and Nash equilibrium, which may not be valid and/or feasible for current and emerging cloud infrastructures because they do not cover some realistic attack scenarios. For examples, their models are not scalable with the realistic sizes and complexity of the infrastructures under consideration, and they assume that the actions of players (both attackers and defenders) are synchronous [4-7]. Another serious limitation of these approaches [4-6] is that it is difficult for game theory models to capture probabilistic human behaviors accurately.

Much research has been done to develop effective approaches to protecting the critical cloud infrastructures [13, 14] and power systems [15-19]. In [13], a technique was presented to leverage the elasticity and on-demand provisioning features of the critical cloud infrastructures to provide application resilience to failures and attacks. In [14], a technique to develop an automated security compliance tool for critical cloud infrastructures was presented. This technique reduces human intervention by verifying the security compliance automatically based on the data collected from API, vulnerability scanning, log analysis and manual input entries. Both techniques [13, 14] are reactive in nature and require all the used security mechanisms being actively applied all the time.

In recent years, organizations [13-19], especially those in the energy sector [15-19], have been adopting probabilistic techniques to proactively predict security breaches for better defense of their infrastructures. The technique presented in [15, 16] has been incorporated in supervisory control and data acquisition (SCADA) systems of energy infrastructures, and uses a probabilistic inference engine to predict potential attack paths by estimating the probability of the occurrence of each attack within one-week period based on the domain knowledge of a professional penetration tester. However, this technique is not suitable for critical cloud infrastructures because its estimates are computationally complex and valid only for a single week. In [17], a technique was presented to estimate the probabilities of potential attacks on energy infrastructures by generating the attack graph using a probabilistic inference engine, but it cannot recognize different instances of the same attack which may be correlated with previous or simultaneous attacks. In [18], a technique was presented to ensure the power transmission systems remain at the acceptable reliability levels with various loads. In doing so, it predicts the loads on various generators and the random failures of system equipment. However, this technique only models the probabilistic characters of power systems with no conflicts between deterministic and probabilistic criteria in transmission planning process. The result of this technique helps save investment in planning while maintaining the acceptable system reliability level**.**

A thread-driven quantitative mathematical framework, called Three Tenets, was developed for secure cyber-physical system design and assessment by predicting attacks using Bayesian network [19], but not involving human behaviors. An approach to situation assessment was developed for helping decision makers in intelligent operations and large-scale crisis management using Bayesian and Credal networks [20]. This approach is not applicable for cases which exceed the cognitive capability of a single expert. A probabilistic reasoning modelling technique was developed using stochastic Petri Nets to understand the tradeoff between information security and operational performance in parallel distributed application environments focusing on moving target defense and deceptive defense tactics [21]. This technique generates a more secure platform by increasing the ratio of deceptive to operational nodes by changing the attack surface (the points of contact of attackers). However, it does not consider an attacker model to be self-aware of when the nodes transition will take place. Instead, this technique relies on the required operational cost.

All these approaches do not incorporate human factors, and hence the predictive capability is limited. In the following,

we will introduce an approach to efficient incorporation of human behaviors to capture the probabilistic human behaviors, and hence provide better predictive capability.

IV. AN APPROACH

In this section, we will discuss a possible approach to quantitatively predicting imminent security breaches on critical cloud infrastructures. This approach will use probabilistic techniques, such as Bayesian network and MDP to predict system-wide security breaches based on the probabilistic inputs on subsystem level security breaches. The approach will be time based, and generate probabilistic predictions of system-wide and sub-system security breaches with the respective time windows, in which breaches are most likely to occur. The domain expert will analyze the network of the critical cloud infrastructure accurately, and provide the information to the state construction algorithms. Since the input from the domain expert to a critical cloud infrastructure is confidential, a data specification language needs to be developed to facilitate the domain expert to provide the sensitive input.

A critical cloud infrastructure may have multiple subsystems and the number of subsystems is determined by the application (domain knowledge). Each subsystem may or may not be connected to other subsystems directly. The only requirement for the critical cloud infrastructure is that each subsystem has the ability to communicate with the Bayesian network, either directly or indirectly. The system-wide Bayesian network can run on a centralized system or a subsystem connected to all the subsystems. The Bayesian network will monitor all the events which occur across subsystems, and predict system-wide security breaches using our approach, which can be summarized as follows:

Step 1) Based on the system state dependencies of the critical cloud infrastructure (identified from the domain knowledge of the application of the critical cloud infrastructure), construct and evaluate the system-wide Bayesian network [22] and the state graphs of the subsystem Markov decision processes (MDP) [23]. The domain expert determines the threshold for the probability of occurrence of each known security breach.

Step 2) Monitor the operations of the critical cloud infrastructure to observe operational behavior which includes the human behaviors, and update the MDP and Bayesian state graphs [generated in ***Step 1)***] based on the causal importance of the observed operational behaviors to security breaches using BPEA and MPEA algorithms, which will be discussed in Section VI.

Step 3) Check the conformance of the Bayesian network structure with Bayesian properties, MDP state graph structure with Markovian properties and also to each other, and update the Bayesian network and MDP state graphs

Step 4) Estimate the accuracy of the state graph metrics of both MDP and Bayesian network. Then find all possible security breaches in the target critical cloud infrastructure and their causal relationship by passively deploying the MDP and the Bayesian network of the infrastructure and then intentionally introducing known vulnerabilities. Loop ***Steps 2)*** to ***4)*** until the estimated accuracy reaches the threshold.

Step 5) Run the MDP and Bayesian network inference engine to predict security breaches at subsystem level and system-wide level, respectively, along with a time window [24, 25]. If the probability of a predicted security breach exceeds the specified threshold for the security breach, the security breach is predicted to occur soon.

Incorporation of probabilistic human behaviors in ***Step 2)*** of our approach, and the involvement of the domain experts in ***Step 1)*** which is off-line, enables our approach to address challenge **C1*).*** Since our approach does not affect the critical cloud operations directly (by not locking many processes of the critical cloud infrastructures), and because the predictive nature of our approach enables the system to selectively apply those security measures based on predicted breaches, the operational overhead of using our approach may not be more than that of existing approaches without predictive capability. This will help address challenge **C3*)***.

Challenge **C2)** is not addressed in our approach, but it can be reduced by incorporating fail-safe mechanisms, such as controller hardening, and robust policy framework [26].

V. PARTIAL ILLUSTRATION

In this section, we will illustrate a part of our approach using the part of the operations for handling online personal transactions in a bank. The critical cloud infrastructure for this part is shown in Figure 1, and it consists of the four subsystems: Subsystem 1 provides the interface of the bank for personal transaction services to all the customers only. In addition, Subsystem 1 also checks possible attack from customers' inputs, such as DoS, CSRF, XSS and SQL injections, but it does not store customers' identity and personal transaction data. To provide better security protection for the customers' data, Subsystem 2 stores anonymized customers' transaction data. Subsystem 3 stores customers' identity data, validates the requests, processes transactions and sends the anonymized transaction data for storage in Subsystem 2. Subsystem 4 performs business analysis of customers' transaction data for bank employees using the anonymized customers' data in Subsystem 2. The bank employees can only access the critical cloud infrastructure using Subsystem 4. Each subsystem of the

critical cloud infrastructure is assumed to have the capability to deploy its own layered security protection mechanisms, such as Firewall, IDS, and antivirus, to protect itself from attacks and to limit the security breaches within the subsystem. When a customer's request for a personal transaction arrives, Subsystem 1 sends the customers' request to Subsystem 3 to verify the validity of the request and perform the transaction if the request is valid, or reject the request if not valid. Subsystem 3 updates the corresponding anonymized transaction data in Subsystem 2. Subsystem 4 retrieves the anonymized transaction data from Subsystem 2 for performing business analysis of the customer's transaction for bank employees. Note that neither the bank employees, nor the customers have direct access to Subsystem 3 which is the only subsystem containing de-anonymized transaction data.

In ***Step 1),*** the initial system state dependencies of the critical cloud infrastructure are identified and the domain expert sets the threshold for the probability of occurrence of each known security breach to 0.8. Construct and evaluate the state graph of MDP and the Bayesian network. Then, predict all the possible security breaches based on the initial information.

In ***Step 2),*** the system state dependencies of the critical cloud infrastructure are monitored and the probabilities of the elements in the MDP and Bayesian network are updated.

In ***Step 3),*** the conformance of the state graph structure of the MDP and the Bayesian network structure are validated.

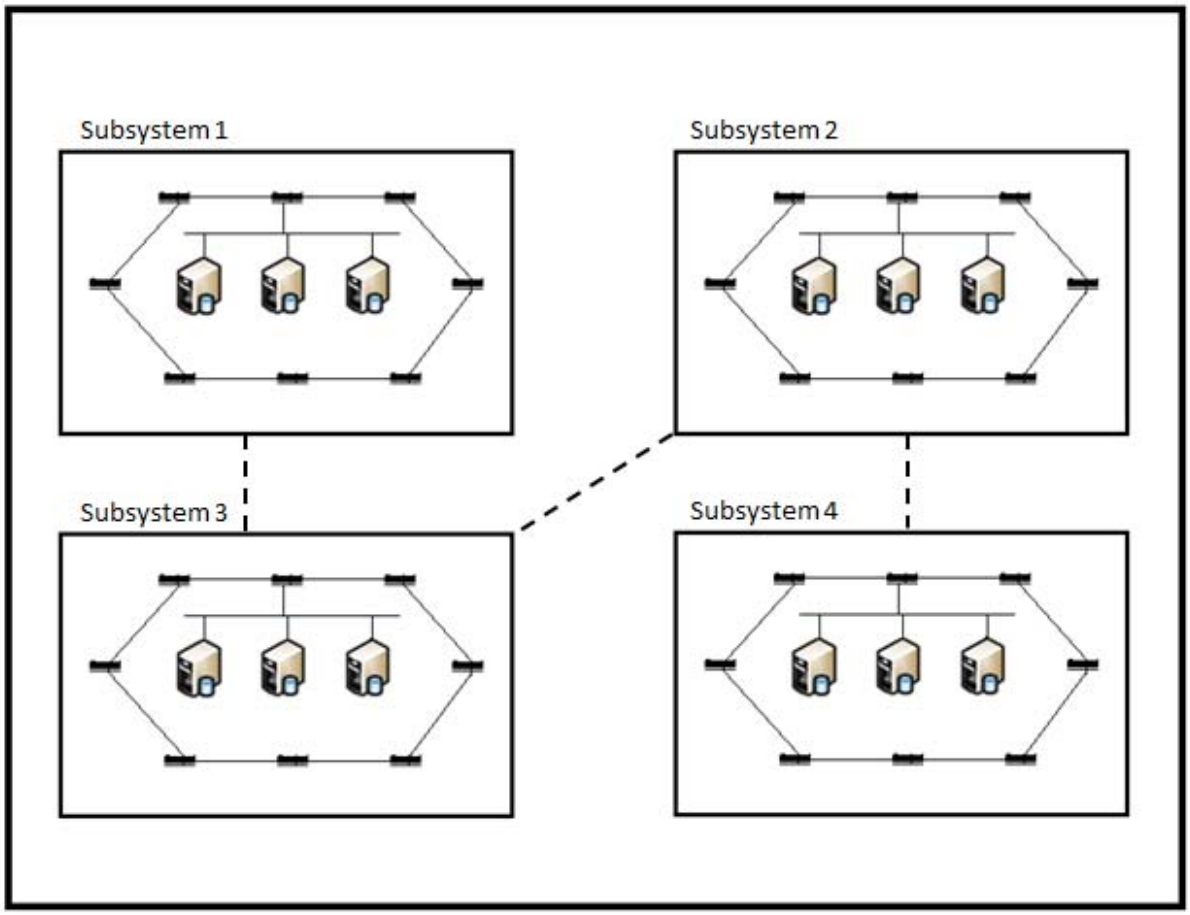

Figure 1: The critical cloud infrastructure for a banking application with MDP running in each subsystem.

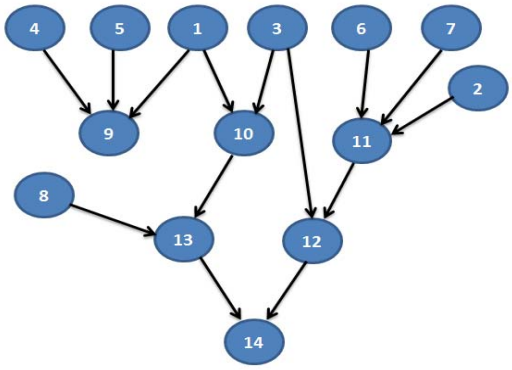

Figure 2: The system-wide Bayesian network for the critical cloud infrastructure of the banking application.

In ***Step 4),*** estimate the accuracy of the state graph metrics and find all possible security breaches of the critical cloud infrastructure. ***Steps 2)*** to ***4)*** continuously run until the accuracy threshold is reached. Figure 2 shows the Bayesian network, where the nodes represent the predicted security breaches and the links represent the causal relationship among the predicted security breaches. In Figure 2, nodes 1 - 8 represent all the possible predicted subsystem security breaches and nodes 9 - 14 represent all the possible predicted system-wide security breaches.

In ***Step 5),*** run all 4 MDPs and the Bayesian network inference engine in the critical cloud infrastructure. If the probability of any node in Figure 2 exceeds 0.8 [the threshold determined by the domain expert in ***Step 1)***], the node is identified as a predicted security breach, which will occur soon.

VI. FURTHER RESEARCH

In order to achieve our vision, the following research needs to be done:

- Develop an effective data specification language for domain experts to provide their input in our approach.
- Generate the probability metrics for the causal relationship among security breaches in Bayesian network, and state dependencies among the states in the MDP.
- Develop effective techniques to construct, check and update the Bayesian network and the state graphs of the MDP using an efficient graph checker algorithm (GCA).
- Develop an efficient way for frequent updating the state graph structures of the MDP and Bayesian network. This is important because of the large amount of computation involved in probabilistic techniques.

In addition, we need to study the feasibility of including additional states in the Bayesian network of the critical cloud infrastructure. This may improve the accuracy of predicted security breaches. Existing research on the intelligent planning for IoT and optimized tradeoff functions [27-29] can be leveraged for this study.

Substantial research is also needed to accurately estimate the probability metrics of the Bayesian network and the state graphs of the MDP. The idea here is to use the past system behavior, human behaviors and situational awareness [30] information to generate probability metrics of the state graphs of the MDP. Since the properties of the Bayesian network and MDP are different, two new algorithms, namely Bayesian probability estimation algorithm (BPEA) and MDP probability estimation algorithm (MPEA), are needed to generate the probability metrics. The BPEA can use the information of system-wide behavior, such as state transitions, security breach occurrences, and the system-wide situational awareness to generate the probability metrics for the Bayesian network. The MPEA can use specific past human behavioral inputs and situational awareness information to estimate the probability metrics of the MDP state graphs in the sub-systems. The probability metrics for both the Bayesian networks and MDP state graphs will be updated frequently so that the state information of the system is current. The BPEA and MPEA can be developed by using the existing approaches [31].

VII. REFERENCES

1. Biggest ever cyber-attacks by Telegraph, "http://www.telegraph.co.uk/technology/internet-security/10848707/The-biggest-ever-cyber-attacks-and-security-breaches.html", Accessed on February 15th, 2015

2. Akhil Behl, "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation", Proceedings of IEEE World Congress on Information and Communication Technologies (WICT), 2011, pp: 217 – 222

3. "Understanding security through probability," by Cisco, "http://blogs.cisco.com/security/understanding-security-through-probability", Accessed on February 15th, 2015

4. Sajjan Shiva, Sankardas Roy, and Dipankar Dasgupta. "Game theory for cyber security." Proceedings of the Sixth Annual Workshop

on Cyber Security and Information Intelligence Research, p. 34. ACM, 2010.
5. Peng Liu, and Lunquan Li. “A Game Theoretic Approach to Attack Prediction.” Technical Report, PSU-S2-2002-001, Penn State Cyber Security Group, 2002.
6. Sankardas Roy, Charles Ellis, Shiva Sajjan, Dipankar Dasgupta, Vivek Shandilya, and Qishi Wu. "A survey of game theory as applied to network security." Proceedings of System Sciences (HICSS), 2010 43rd Hawaii International Conference on, pp. 1-10. IEEE Press2010
7. Milind Tambe, Manish Jain, James Adam Pita, and Albert Xin Jiang. "Game theory for security: Key algorithmic principles, deployed systems, lessons learned." Proceedings of Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on, pp. 1822-1829. IEEE Press, 2012.
8. Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacşar, and Jean-Pierre Hubaux. "Game theory meets network security and privacy." ACM Computing Surveys (CSUR) 45, no. 3 (2013): 25.
9. Alecsandru PĂTRAŞCU, and Emil Simion. "Game theory in cyber security defence." Proceedings of Electronics, Computers and Artificial Intelligence (ECAI), 2013 International Conference on, pp. 1-6. IEEE Press, 2013.
10. Dan Shen, Genshe Chen, Jose B. Cruz Jr, Leonard Haynes, Martin Kruger, and Erik Blasch. "A markov game theoretic data fusion approach for cyber situational awareness." Proceedings of Defense and Security Symposium, pp. 65710F-65710F. International Society for Optics and Photonics, 2007.
11. Dan Shen, Genshe Chen, Leonard Haynes, and Erik Blasch. "Strategies comparison for game theoretic cyber situational awareness and impact assessment." Proceedings of Information Fusion, 2007 10th International Conference on, pp. 1-8. IEEE Press, 2007.
12. Wei Jiang, Zhi-hong Tian, Hong-li Zhang, and Xin-fang Song. "A stochastic game theoretic approach to attack prediction and optimal active defense strategy decision." Proceedings of 2008 IEEE International Conference on, Networking, Sensing and Control, pp. 648-653. 2008.
13. Azzedine Benameur, Nathan S. Evans, Matthew C. Elder, “Cloud resiliency and security via diversified replica execution and monitoring”, Proceedings of 2013 6th International Symposium on Resilient Control Systems (ISRCS), 2013 , pp: 150- 155
14. Ullah K.W., Ahmed A.S., Ylitalo J., “Towards Building an Automated Security Compliance Tool for the Cloud”, Proceedings of Trust, Security and Privacy in 2013 12th IEEE International Conference on Computing and Communications (TrustCom), , pp: 1587- 1593
15. Teodor Sommestad, "A framework and theory for cyber security assessments." PhD diss., KungligaTekniskahögskolan (KTH), Royal Institute of Technology Stockholm, Sweden, 2012.
16. Teodor Sommestad, Mathias Ekstedt, and Lars Nordström, "A case study applying the Cyber Security Modeling Language.", Proceedings of CIGRE 2010.
17. Holm Hannes, Khurram Shahzad, Markus Buschle, and Mathias Ekstedt, "CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language.", IEEE Transactions onDependable and Secure Computing,, vol. 99, 2014, pp.1,1.
18. Wenyuan Li, and P. Choudhury. "Probabilistic planning of transmission systems: Why, how and an actual example.", Proceedings of 21st IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy the 21st Century, 2008, pp. 1-8.
19. Jeff Hughes, and George Cybenko, "Three tenets for secure cyber-physical system design and assessment.", Proceedings of Society of Photo-Optical Instrumentation Engineers Defense Security, June, 2014
20. Claudine Conrado and Patrick de Oude, "Scenario-based reasoning and probabilistic models for decision support.", Proceedings of 17th IEEE Information Fusion (FUSION), July, 2014, pp. 1-9.
21. W.C. Moody, Hongxin Hu, A. Apon, "Defensive maneuver cyber platform modeling with Stochastic Petri Nets,", Proceedings of 10th International Conference on Collaborative Computing (CollaborateCom 2014), October 22-25, 2014.
22. Moninder Singh and Marco Valtorta. "Construction of Bayesian network structures from data: a brief survey and an efficient algorithm." International journal of approximate reasoning 12, no. 2 (1995): 111-131.
23. Puterman, Martin L. “Markov decision processes: discrete stochastic dynamic programming.” John Wiley & Sons, 2014.
24. Catharine McGhan, Ali Nasir, and Ella Atkins. "Human intent prediction using markov decision processes.", Proceedings of Infotech@ Aerospace 2012 (2012): 2.
25. Ehsan Nazerfard and Diane J. Cook. "Using Bayesian Networks for Daily Activity Prediction,” Proceedings of the 14th Conf. in Uncertainty in Artificial Intelligence, 480–487.
26. Diego Kreutz, Fernando Ramos, and Paulo Verissimo. "Towards secure and dependable software-defined networks." Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, pp. 55-60. ACM, 2013.
27. S. S. Yau and A. B. Buduru, "Intelligent Planning for Developing Mobile IoT Applications Using Cloud Systems", Proceedings of 3rd IEEE International Conference on Mobile Services (MS), June 2014, pp. 55-62
28. S. I. Ahamed, I. Addo, S. S. Yau, and A. B. Buduru, "A Reference Architecture for Improving Security and Privacy in Internet of Things Applications", Proceedings of 3rd IEEE International Conference on Mobile Services (MS), June 2014, pp. 108-115
29. S. S. Yau, Y. Yin, and H. G. An, “An Adaptive Approach to Optimizing Tradeoff between Service Performance and Security in Service-based Systems”, International Journal of Web Services Research, Vol. 8(2), 2011, pp. 74-91.
30. S. S. Yau, D. Huang, "Development of Situation-Aware Applications in Services and Cloud Computing Environments", International Journal of Software and Informatics, Vol 7(1), 2013, pp. 21-39.
31. Adlakha Sachin, Sanjay Lall, and Andrea Goldsmith. "A Bayesian network approach to control of networked Markov decision processes." Proceedings of 46th IEEE Conference on Communication, Control, and Computing, 2008, pp. 446-451.