Applications of Security Reference Architectures in Distributed Systems: Initial Findings of Systematic Mapping Study

Sajjad Mahmood, Muhammad Jalal Khan and Sajid Anwer
Information and Computer Science Department
King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia
e-mail: [smahmood, g201408880, g201303950]@kfupm.edu.sa

***Abstract*—There is an increase in use of reference architectures to support software development activities for building distributed systems. Reference architectures are helpful tools to understand and specify functionalizes of a distributed system at a higher abstraction level. From a security standpoint, a distributed system's reference architecture is one of the potential starting point to study security threats and their characteristics. Both academia and industry have proposed a number of Security Reference Architectures (SRAs), which are reference architectures specifying a conceptual model of security for a system and they provide a mechanism to specify security requirements. The main objective of this work is to investigate and better understand how security reference architecture support building secure distributed software applications. In order to meet our goal, we conducted a systematic mapping study to identify the primary studies related to SRA for distributed software development. We used customized search terms, derived from our research question, to identify literature on SRA for distributed systems. We identified that a significant number of SRAs have been developed first for defense against one or few specific types of security attacks. There is also a focus on developing SRAs to satisfy a security objective during development of distributed systems. Based on the systematic mapping study results, we suggest that there is a need to develop SRAs that help system developers simultaneously enumerate different types of security threats and systematically help to decide where we should add corresponding security patterns to mitigate them.**

Keywords-security reference architecture; reference architecture; distributed systems; systematic mapping study.

I. INTRODUCTION

The past several years have seen tremendous changes in distributed software development due to introduction of web 2.0 technologies [14], service oriented architectures [15] and cloud computing systems [16]. These distributed system development technologies have brought with them several new and complex security threats and challenges. To holistically study security of these large and complex distributed systems, we need to start our security analysis from their security reference architectures [1].

A security reference architecture is a reference architecture where security mechanisms have been added in appropriate places to provide some degree of security [1]. Furthermore, a reference architecture is an abstract system architecture that describes system functionalities without any implementation details [1]. Reference architectures are useful to specify main features of a system.

A number of SRAs have been proposed by both academia and industry vendors. For example, Chonka et al. [2] report a technique that is used to observe and discover denial of service attacks against cloud systems. Okuhara et al. [3] report Fujitsu's security architecture, which logically separates computational environments, authentication and identify management. Similarly, Oracle developed a SRA [4], which addresses data security, fraud detection and compliance with reference to their products.

The literature on SRAs provides a wealth of information on how to analyze security of a system for individual attacks, model system for a security objective(s) or how to help systems meet security compliance requirements of a government organization. For example, Bahmani et al. [5] compared different enterprise information security architecture frameworks with reference to interoperability feature. Lately, Modi et al. [6] presented a survey of intrusion detection techniques in cloud computing systems.

However, there is a lack of systematic investigation of the literature covering SRA in distributed systems. The aim of this systematic mapping study is to collate knowledge to better understand how SRAs have supported system security and identify in what ways it has been applied in the industry.

The remaining of this paper is organized as follows: Section II presents the related work. The research methodology is outlined in Section III. In Section IV, we present and discuss the initial results. Section V discusses the limitation of our study. Finally, the conclusion is presented in Section VI.

II. RELATED WORK

Security is a fundamental concern in any distributed system and a number of security reference architectures have been proposed by industry and researchers' community. Majority of security reference architectures have been proposed for a particular attack type. There has been significant focus on developing SRAs to mitigate attacks such as denial of service [22], Internet protocol spoofing and denial of service [23].

On the other hand, researchers have also focused on developing security objective specific SRA. For example, Hafner et al. [10] have used enterprise patterns to develop secure services for cloud computing systems. Lombardi and Pietro [11] used virtualization to propose an architecture for cloud protection that monitors middleware integrity.

Even though extensive research has been carried out in the security reference architecture domain, it is necessary to

 ISBN: 978-1-61208-438-1

assess the current state of research and practice, and provide practitioners with evidence that enables fostering future research directions. To the best of our knowledge, there is a lack of systematic investigation of the literature covering SRA in distributed systems.

III. RESEARCH METHODOLOGY

In order to address the research question, we applied Systematic mapping study and literature review [7] approach. A systematic mapping study and literature review is a technique to identify, analyze and interpret relevant published primary studies with reference to a specific research question. Systematic mapping studies are recommended as a review methodology [7] because they allow the researchers to systematically summarize existing evidence from literature, identify research gaps and provide a framework to position future research activities [13].

A systematic mapping study protocol consists of five main phases, as shown in Figure 1. In the first phase of our study, we formulated a research question as follows:

RQ1: How is security reference architecture supporting development of distributed systems?

Next, we constructed the search strategy in line with our research question and performed the search for relevant publications. In the third phase, the identified relevant publications were scrutinized to ensure their relevance. In the fourth phase, the selected studies were evaluated based on the quality assessment criteria. In the last phase, data was extracted from selected studies for further analysis and assessment.

A. Search Strategy

The search strategy for the systematic mapping study is based on the steps as follows:

- Derive the search terms from population, intervention and outcomes.
- Identify alternative spellings and synonyms for major terms.
- Use Boolean 'OR' and 'AND' operators.
- Verify the derived search term in major academic repositories.

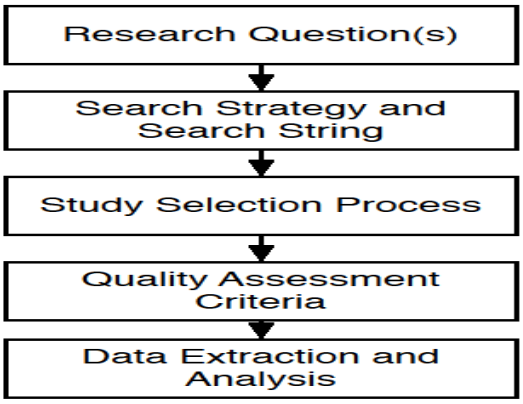

Figure 1. Systematic Mapping Study Major Process Phases.

We constructed the following search terms based on our search strategy:

- POPULATION: Distributed systems, Cloud systems, Service-oriented Architecture.
- INTERVENTION: Security Methodology.
- OUTCOME OF RELEVANCE: Different techniques to mitigate security in reference architecture, classification of SRAs.
- EXPERIMENTAL DESIGN: Systematic literature reviews and empirical studies.

We validated our search terms in major academic databases in a scoping study. The following search terms show potential relevance to the research question as follows:

- SECURITY REFERENCE ARCHITECTURE: Security Architecture OR Security Reference Architecture OR Security Design OR Security Architecture Design, Security Patterns; AND
- DISTRIBUTED SYSTEM: Distributed Systems OR Cloud Systems OR Service-oriented Architecture OR Grid Systems; AND
- TECHNIQUE: Technique OR Method OR Model OR Design.

The relevant studies retrieved through the initial search string were used as a guide for the development and validation of the final search string. In the scoping study, we used some relevant publications, which we had previously identified to cross check the validity of the search terms. A broad search was conducted between February 2015 and May 2015 to identify relevant articles published (or available on-line) up to May 2015.

B. Publication Selection

The following inclusion criteria were used:

- Peer-reviewed studies.
- Papers focus on answering our research question.
- Papers published in English.

We applied the exclusion criteria as follows:

- Papers that are not published in English.
- Papers with no link with the research question.
- Grey publications, that is, papers without bibliographic information.
- In the case of duplicate papers, the most complete version published.

Next, each paper was evaluated against the quality assessment criteria shown in Table 1. Each quality assessment criterion has two answers: 'Yes' or 'No' with scores of '1' and '0', respectively. The sum of the quality criteria resulted in the quality score for a particular paper. In this study, we only consider publications with a quality score greater than 75%. As a result, 58 papers were finally selected, which met the inclusion and quality assessment criteria.

 ISBN: 978-1-61208-438-1

TABLE I. QUALITY ASSESSMENT

Quality Criteria	Possible Answers
Is there a rationale for why the study was undertaken? [8]	Yes =1 No =0
Are the research goals clearly stated?	Yes =1 No =0
Is the proposed technique clearly described?	Yes =1 No =0
Is the research empirically validated?	Yes =1 No =0
Are the limitations of this study explicitly discussed? [9]	Yes =1 No =0
Is the study supported by a tool?	Yes =1 No =0

Initially, when synthesizing the data, data was extracted from the final selection of papers as follows: study details, study research methodology, assessment details and study findings.

IV. RESULTS AND DISCUSSION

The total number of results retrieved using the search terms in the electronic databases are shown in Table 2. After the initial round of screening by reading the title and abstract, seventy one studies belonging to different electronic research databases were selected. After full text readings in the second screening and quality assessment, 58 primary studies were finally selected. Figure 2 shows temporal view of the selected articles from the systematic review, sorted by year of publication. Appendix A presents the primary studies in the review.

TABLE II. SEARCH EXECUTION

Resource	Total Results	Initial Selection	Final Selection
ACM	200	11	10
IEEE Xplore	427	36	27
Science Direct	350	18	15
Springer	61	6	6
Total	1038	71	58

To answer the research question, the data was carefully extracted and synthesized from the 58 finally selected primary studies. We classified SRAs into four main categories as shown in Table 3.

In our study, the most highly cited category is 'attack specific SRA' (60%). Distributed system infrastructure uses virtualization techniques and provide their services through standard internet protocols [6]. Distributed systems are vulnerable to traditional security attacks such as Internet protocol spoofing, routing information protocol attacks, denial of service attacks, etc. Hence, there has been a significant focus on developing SRAs to incorporate specific attack detection and prevention mechanisms in distributed system infrastructure to mitigate security attacks. Table 4 shows a list of popular types of attacks addressed by researchers and industry practitioners.

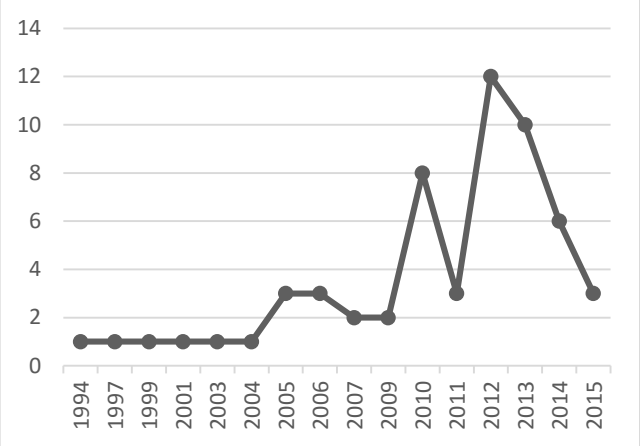

Figure 2. Temporal view of studies

'Security objective specific SRA' is the second highly cited category (reported by 34 % of the articles selected from the systematic mapping study and review). Researchers have also considered developing SRAs oriented to some specific security objectives. For example, Hafner et al. [10] have used enterprise patterns to develop secure services for cloud computing systems. Lombardi and Pietro [11] used virtualization to propose an architecture for cloud protection that monitors middleware integrity. Lately, Fernandez et al. [1] presented a method to build a SRA for cloud systems using security patterns and misuse patterns.

TABLE III. LIST OF SRAS CATEGORIES

Categories	Studies	Count	%
Attack Specific SRA	A1, A3, A4, A5, A6, A7, A8, A9, A10, A11, A12, A13, A15, A17, A18, A21, A23, A24, A25, A27, A28, A30, A37, A39, A40, A41, A42, A46, A47, A49, A53, A54, A55, A57, A58	35	60.30
Security Objective Specific SRA	A2, A14, A19, A22, A29, A31, A32, A33, A34, A35, A36, A38, A43, A44, A45, A48, A50, A51, A52, A56	20	34.48
Industry Specific SRA	A21, A26	2	3.44
Vendor Specific SRA	A16	1	1.72

Furthermore, less frequently cited categories are 'industry specific SRA' and 'vendor specific SRA. There has been couple of SRAs developed for a specific industry. For example, Cohen [12] developed a SRA for industrial control systems. Similarly, Bahmani et al. [5] discussed five enterprise security reference architectures, namely, Gartner

 ISBN: 978-1-61208-438-1

framework [17], SABSA [18], roadmap for information security across the enterprise framework [19], agile governance model based model [20] and intelligent service-oriented enterprise security architecture [21].

TABLE IV. LIST OF POPULAR TYPES OF ATTACKS

Attack Type	%
Authentication/Authorization	45
Denial of Service	22
Injection	20
Denial of Service	20
Man in the Middle Attack	14
Data Tempering	11
Brute Force	5

It is important to note that over the years, a significant number of SRAs have been developed by industry vendors. All major industrial vendors like IBM, Microsoft, Oracle, Cisco, VMware and Amazon have developed SRAs for their product range. However, in our study, we have not included them as primary studies because most of vendor specific SRAs are available in form of white papers, which do not satisfy our inclusion criteria, as mentioned in Section 2. Hence, we have included only on primary study regarding Fujistu's SRA reported by Okuhara et al. [3].

V. LIMITATIONS

Similarly to any systematic mapping study and literature review, our results also depend on the used keywords and the limitations of the search engines. In order to limit the risk of incompleteness in keywords lists, we used alternative spellings and synonyms to build the search terms.

Application of inclusion, exclusion criteria and primary study selection process are also subject to threats to validity of the study. In order to mitigate this threat, all systematic mapping study phases were carried out iteratively with continuous feedback from authors of the paper.

VI. CONCLUSIONS AND FUTURE WORK

In this paper, we conducted a systematic mapping study to investigate the use of SRA to support development of distributed systems. Fifty eight studies were finally included, which were further classified into four categories, namely, 'attack specific SRA', 'security objective specific SRA', 'industry specific SRA' and 'vendor specific SRA'.

Through this systematic mapping study, we identified that researchers have mainly focused on developing SRAs for one or group of individual security attacks. There also has been a focus on developing SRAs oriented to security objectives such as monitoring data and using security patterns to add security mechanisms at appropriate components of a system.

We believe that the results presented in our systematic mapping study and review can be useful for software engineering community as it provides an initial body of knowledge regarding SRAs. In the future, we intend to expand this systematic review to further analyze individual categories and discuss highly cited types of attacks and security objectives in the literature. Another area for future work is to empirically study different industry vendor SRAs and their impact on improving security of distributed systems.

ACKNOWLEDGMENT

The authors would like to thank King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia for continuous support in research. This research is supported by the Deanship of Scientific Research at KFUPM under research grant IN131013.

REFERENCES

[1] E. B. Fernandez, R. Monge, and K. Hashizume, "Building a security reference architecture for cloud systems," Requirements Engineering, 2015, pp. 1-25.

[2] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," Journal of Network and Computer Applications, vol. 34, 2011, pp. 1097-1107.

[3] M. Okuhara, T. Shiozaki, and T. Suzuki, "Security architecture for cloud computing," Fujitsu Sci. Tech. J, vol. 46, 2010, pp. 397-402.

[4] M. Wilkins, "Orcale Reference Architecture: Cloud Foundation Architecture " Technical Report E24529-01 - Orcale Corporation, 2011.

[5] F. Bahmani, M. Shariati, and F. Shams, "A survey of interoperability in Enterprise Information Security Architecture frameworks," in Information Science and Engineering (ICISE), 2010 2nd International Conference on, 2010, pp. 1794-1797.

[6] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A Survey of Instrusion Detection Techniques in Cloud," Journal of Network and Computer Applications, vol. 36, 2013, pp. 42-57.

[7] B. Kitchenham and C. Charters, "Guidelines for Performing Systematic Literarature Reviews in Software Engineering," Keele University and Durham University Joint Report, 2007.

[8] S. Mahdavi-Hezavehi, M. Galster, and P. Avgeriou, "Variability in quality attributes of service-based software systems: A systematic literature review," Information and Software Technology, vol. 55, 2013, pp. 320-343.

[9] W. Ding, P. Liang, A. Tang, and H. Van Vliet, "Knowledge-based approaches in software documentation: A systematic literature review," Information and Software Technology, vol. 56, 2014, pp. 545-567.

[10] M. Hafner, M. Memon, and R. Breu, "SeAAS - A Reference Architecture for Security Services in SOA," Journal of Universal Computer Science, vol. 15, 2009, pp. 2916-2936.

[11] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," Journal of Network and Computer Applications, vol. 34, 2011, pp. 1113-1122.

[12] F. Cohen, "A Reference Architecture Approach to ICS Security," presented at the 4th International Symposium on Resilient Control Systems, 2011, pp. 9-11.

[13] J. M. Verner, O. P. Brereton B. A. Kitchenham, M. Turner, and M. Niazi, "Systematic Literature Reviews in Global Software Development: A Tertiary Study" in proceedings of the 16th International Conference on Evaluation and Assessment in Software Engineering, 2012, pp. 2-11.

[14] U. Sivarajah, Z. Irani, and S. Jones, "Application of Web 2.0 Technologies in E-Government: A United Kingdom Case Study", in proceedings of 7th Hawaii Inernational Conference on System Sciences, 2014, pp. 2221-2230.

[15] D. Krafzig, K. Banke, and D. Slama, "Enterprise SOA: Service-Oriented Architecture Best Practices", Pearson Education, 2005.

[16] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications and Approaches", Wireless Communications and Mobile Computing, vol. 13, 2013, pp. 157-1611.

 ISBN: 978-1-61208-438-1

[17] T. Scholtz, "Structure and Content of an Enterprise Information Security Architecture", Gartner, 2006.

[18] J. Sherwood, A. Clark, and D. Lynas, "Enterprise Security Architecture: A Business-Driven Approach", CMP Books, 2015.

[19] J. A. Aderson and V. Rachamadugu, "Managing Security and Privacy Integration Across Enterprise Business Process and Infrastrucutre", in proceedings of IEEE International Conference on Service Computing, 2008, pp. 351-358.

[20] J.J. Korhonen, M. Yildiz, and J. Mykkanen, "Governance of Information Security Elements in Service-Oriented Enterprise Architecture in Pervasive Systems", in proceedings of 10th International Symposium on Algorithms and Networks, 2009, pp. 768-773.

[21] J. Sun and Y. Chen, "Intelligent Enterprise Information Security Architecture Based on Service Oriented Architecture", in proceedings of International Semiar on Future Information Technology and Management Engineering, 2008, pp. 196-200.

[22] W. Itani and A. Kayssi, "SPECSA: a scalable, policy-driven, extensible, and customizable security architecture for wireless enterprise applications," Computer Communications, vol. 27, 2004, pp. 1825-1839.

[23] G. Yang et al., "Analysis of security threats and vulnerability for cyber-physical systems," in proceeding of 3rd International Conference on Computer Science and Network Technology (ICCSNT), 2013, pp. 50-55.

APPENDIX A: SYSTEMATIC MAPPING STUDY PRIMARY STUDIES

A1: S. Muftic and M. Sloman, "Security architecture for distributed systems," Computer Communications, vol. 17, pp. 492-500, 1994.

A2: M. Moriconi, Q. Xiaolei, R. A. Riemenschneider, and G. Li, "Secure software architectures," in Security and Privacy, 1997.

A3: R. Molva, "Internet security architecture," Computer Networks, vol. 31, pp. 787-804, 1999.

A4: M. S. Olivier, "Towards a configurable security architecture," Data and Knowledge Engineering, vol. 38, pp. 121-145, 2001.

A5: V. Varadharajan and D. Foster, "A Security Architecture for Mobile Agent Based Applications," World Wide Web, vol. 6, pp. 93-122, 2003/03/01 2003.

A6: W. Itani and A. Kayssi, "SPECSA: a scalable, policy-driven, extensible, and customizable security architecture for wireless enterprise applications," Computer Communications, vol. 27, pp. 1825-1839, 2004.

A7: M. Debbabi, M. Saleh, C. Talhi, and S. Zhioua, "Security Analysis of Mobile Java," in Database and Expert Systems Applications, 2005. Proceedings. Sixteenth International Workshop on, 2005, pp. 231-235.

A8: D. Gabrijelčič, B. J. Blažič, and J. Tasič, "Future active Ip networks security architecture," Computer Communications, vol. 28, pp. 688-701, 2005.

A9: G. Gousios, E. Aivaloglou, and S. Gritzalis, "Distributed component architectures security issues," Computer Standards & Interfaces, vol. 27, pp. 269-284, 2005.

A10: A. Vorobiev and J. Han, "Secrobat: Secure and Robust Component-based Architectures," in Software Engineering Conference, 2006. APSEC 2006. 13th Asia Pacific, 2006, pp. 3-10.

Proceedings., 1997 IEEE Symposium on, 1997, pp. 84-93.

A11: C. Lu, T. Zhang, W. Shi, and H.-H. S. Lee, "M-TREE: A high efficiency security architecture for protecting integrity and privacy of software," Journal of Parallel and Distributed Computing, vol. 66, pp. 1116-1128, 2006.

A12: T. Fægri and S. Hallsteinsen, "A Software Product Line Reference Architecture for Security," in Software Product Lines, T. Käköla and J. Duenas, Eds., ed: Springer Berlin Heidelberg, 2006, pp. 275-326.

A13: C. Martin and K. A. Abuosba, "Utilizing a Service Oriented Architecture for Information Security Evaluation and Quantification," in Business-Driven IT Management, 2007. BDIM '07. 2nd IEEE/IFIP International Workshop on, 2007, pp. 114-115.

A14: V. S. Sharma and K. S. Trivedi, "Quantifying software performance, reliability and security: An architecture-based approach," Journal of Systems and Software, vol. 80, pp. 493-509, 2007.

A15: R. Shioya, K. Daewung, K. Horio, M. Goshima, and S. Sakai, "Low-Overhead Architecture for Security Tag," in Dependable Computing, 2009. PRDC '09. 15th IEEE Pacific Rim International Symposium on, 2009, pp. 135-142.

A16: M. Okuhara, T. Shiozaki, and T. Suzuki, "Security architecture for cloud computing," Fujitsu Sci. Tech. J, vol. 46, pp. 397-402, 2010.

A17: J. Li, X. Lu, and G. Gao, "A mobile ad hoc network security architecture based on immune agents," in Communication Systems, Networks and Applications (ICCSNA), 2010 Second International Conference on, 2010, pp. 224-227.

A18: S. Donglai, W. Yue, W. Tian, L. Yang, L. Ning, and T. Junhua, "Design and Construction of a Prototype Secure Wireless Mesh Network Testbed," in Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on, 2010, pp. 345-350.

A19: R. G. Addie and A. Colman, "Five Criteria for Web-Services Security Architecture," in Network and System Security (NSS), 2010 4th International Conference on, 2010, pp. 521-526.

A20: H. Xu, F. Wan, H. Zheng, and M. Xu, "A Security Architecture Model of CSCW System," in Management and Service Science (MASS), 2010 International Conference on, 2010, pp. 1-4.

A21: F. Bahmani, M. Shariati, and F. Shams, "A survey of interoperability in Enterprise Information Security Architecture frameworks," in Information Science and Engineering (ICISE), 2010 2nd International Conference on, 2010, pp. 1794-1797.

A22: M. Asgarnezhad, R. Nasiri, and S. Sahebhonar, "Analysis and Evaluation of Two Security Services in SOA," in Internet and Web Applications and Services (ICIW), 2010 Fifth International Conference on, 2010, pp. 562-568.

A23: A. M. Rossudowski, H. S. Venter, J. H. P. Eloff, and D. G. Kourie, "A security privacy aware architecture and protocol for a single smart card used for multiple services," Computers & Security, vol. 29, pp. 393-409, 2010.

A24: G. Dini and I. Savino, "A Security Architecture for Reconfigurable Networked Embedded Systems," International Journal of Wireless Information Networks, vol. 17, pp. 11-25, 2010/06/01 2010.

A25: T. Yuan, S. Biao, and H. Eui-Nam, "Towards the Development of Personal Cloud Computing for Mobile Thin-Clients," in Information Science and Applications (ICISA), 2011 International Conference on, 2011, pp. 1-5.

A26: F. Cohen, "A reference architecture approach to ICS security," in Resilient Control Systems (ISRCS), 2011 4th International Symposium on, 2011, pp. 21-25.

A27: L. Xiaoli, C. Jinhua, and L. Min, "A Simple Security Model Based on Cloud Reference Model," in Distributed Computing and Applications to Business, Engineering and Science (DCABES), 2011 Tenth International Symposium on, 2011, pp. 155-159.

A28: H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," presented at the Proceedings of the 7th International Conference on Body Area Networks, Oslo, Norway, 2012.

A29: D. Allam, "A unified formal model for service oriented architecture to enforce security contracts," presented at the Proceedings of the 11th annual international conference on Aspect-oriented Software Development Companion, Potsdam, Germany, 2012.

A30: A. Sharma, V. Fusenig, I. Schoen, and A. Kannan, "Bridging the security drawbacks of virtualized network resource provisioning model," presented at the Proceedings of the 1st European Workshop on Dependable Cloud Computing, Sibiu, Romania, 2012.

A31: S. Rangarajan, M. Verma, A. Kannan, A. Sharma, and I. Schoen, "V2C: a secure vehicle to cloud framework for virtualized and on-demand service provisioning," presented at the Proceedings of the International Conference on Advances in Computing, Communications and Informatics, Chennai, India, 2012.

 ISBN: 978-1-61208-438-1

A32: Y. F. Wang, W. M. Lin, T. Zhang, and Y. Y. Ma, "Research on application and security protection of Internet of Things in Smart Grid," in Information Science and Control Engineering 2012 (ICISCE 2012), IET International Conference on, 2012, pp. 1-5.

A33: G. Mathew, "Security considerations and reference architecture of a cyber computing infrastructure for online education," in E-Learning, E-Management and E-Services (IS3e), 2012 IEEE Symposium on, 2012, pp. 1-6.

A34: Y. Chenghua, Z. Qi, and Z. Zhiming, "Study on Information Security Assurance Architecture in Internet," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, 2012, pp. 293-296.

A35: J. Montelibano and A. Moore, "Insider Threat Security Reference Architecture," in System Science (HICSS), 2012 45th Hawaii International Conference on, 2012, pp. 2412-2421.

A36: T. Okubo, H. Kaiya, and N. Yoshioka, "Mutual Refinement of Security Requirements and Architecture Using Twin Peaks Model," in Computer Software and Applications Conference Workshops (COMPSACW), 2012 IEEE 36th Annual, 2012, pp. 367-372.

A37: L. Lan, "Study on security architecture in the Internet of Things," in Measurement, Information and Control (MIC), 2012 International Conference on, 2012, pp. 374-377.

A38: J. Li, B. Li, T. Wo, C. Hu, J. Huai, L. Liu, and K. P. Lam, "CyberGuarder: A virtualization security assurance architecture for green cloud computing," Future Generation Computer Systems, vol. 28, pp. 379-390, 2012.

A39: A. Talib, R. Atan, R. Abdullah, and M. Murad, "Ensuring Security and Availability of Cloud Data Storage Using Multi Agent System Architecture," in Knowledge Technology. vol. 295, D. Lukose, A. Ahmad, and A. Suliman, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 343-347.

A40: W. Scacchi and T. A. Alspaugh, "Processes in securing open architecture software systems," presented at the Proceedings of the 2013 International Conference on Software and System Process, San Francisco, CA, USA, 2013.

A41: M. Shtern, B. Simmons, M. Smit, and M. Litoiu, "An architecture for overlaying private clouds on public providers," presented at the Proceedings of the 8th International Conference on Network and Service Management, Las Vegas, Nevada, 2013.

A42: M. Almorsy, J. Grundy, and A. S. Ibrahim, "Automated software architecture security risk analysis using formalized signatures," presented at the Proceedings of the 2013 International Conference on Software Engineering, San Francisco, CA, USA, 2013.

A43: A. Guerrieri, L. Geretti, G. Fortino, and A. Abramo, "A service-oriented gateway for remote monitoring of building sensor networks," in Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2013 IEEE 18th International Workshop on, 2013, pp. 139-143.

A44: W. Ruoyu, Z. Xinwen, A. Gail-Joon, H. Sharifi, and X. Haiyong, "ACaaS: Access Control as a Service for IaaS Cloud," in Social Computing (SocialCom), 2013 International Conference on, 2013, pp. 423-428.

A45: G. Yang, P. Yong, X. Feng, Z. Wei, W. Dejin, H. Xuefeng, L. Tianbo, and L. Zhao, "Analysis of security threats and vulnerability for cyber-physical systems," in Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on, 2013, pp. 50-55.

A46: A. Masood, "Cyber security for service oriented architectures in a Web 2.0 world: An overview of SOA vulnerabilities in financial services," in Technologies for Homeland Security (HST), 2013 IEEE International Conference on, 2013, pp. 1-6.

A47: D. Gros, M. Blanc, J. Briffaut, and C. Toinard, "PIGA-cluster: A distributed architecture integrating a shared and resilient reference monitor to enforce mandatory access control in the HPC environment," in High Performance Computing and Simulation (HPCS), 2013 International Conference on, 2013, pp. 273-280.

A48: L. Zhang, Q. Wang, and B. Tian, "Security threats and measures for the cyber-physical systems," The Journal of China Universities of Posts and Telecommunications, vol. 20, Supplement 1, pp. 25-29, 2013.

A49: A. De Santis, A. Castiglione, U. Fiore, and F. Palmieri, "An intelligent security architecture for distributed firewalling environments," Journal of Ambient Intelligence and Humanized Computing, vol. 4, pp. 223-234, 2013/04/01 2013.

A50: E. B. Fernandez, R. Monge, and K. Hashizume, "Building a security reference architecture for cloud systems," Requirements Engineering, pp. 1-25, 2015.

A51: O. E. C, E. B. Fernandez, Ra, #250, and l. M. A, "Towards Secure Inter-Cloud Architectures," presented at the Proceedings of the 8th Nordic Conference on Pattern Languages of Programs (VikingPLoP), Vihula, Estonia, 2014.

A52: Y. Tonghao and Y. Bin, "Study of cryptography-based cyberspace data security," in Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on, 2014, pp. 1-7.

A53: M. Jouini, L. B. A. Rabai, and A. B. Aissa, "Classification of Security Threats in Information Systems," Procedia Computer Science, vol. 32, pp. 489-496, 2014.

A54: H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic, and D. Svetinovic, "Integrated smart grid systems security threat model," Information Systems, 2014.

A55: S. Sicari, C. Cappiello, F. De Pellegrini, D. Miorandi, and A. Coen-Porisini, "A security-and quality-aware system architecture for Internet of Things," Information Systems Frontiers, pp. 1-13, 2014/11/04 2014.

A56: A. K. Dwivedi and S. K. Rath, "Incorporating Security Features in Service-Oriented Architecture using Security Patterns," SIGSOFT Softw. Eng. Notes, vol. 40, pp. 1-6, 2015.

A57: J. Maerien, S. Michiels, D. Hughes, C. Huygens, and W. Joosen, "SecLooCI: A comprehensive security middleware architecture for shared wireless sensor networks," Ad Hoc Networks, vol. 25, Part A, pp. 141-169, 2015.

A58: P. Karpati, A. L. Opdahl, and G. Sindre, "Investigating security threats in architectural context: Experimental evaluations of misuse case maps," Journal of Systems and Software, vol. 104, pp. 90-111, 2015.

 ISBN: 978-1-61208-438-1