ARTIFICIAL INTELLIGENCE: ROLE & IMPORTANCE IN CYBER SECURITY THREATS - A REVIEW

Razauddin* & Dr. Leena Bhatia**

** Ph. D. Scholar, Himalayan University, Itanagar, Arunachal Pradesh, India.*

***Research Supervisor, Himalayan University, Itanagar, Arunachal Pradesh, India.*

Today's world is a world where it is impossible to avoid computers. In fact, it is called the age of information technology. It is believed that information is floating everywhere. The successful person is able to catch hold of the right piece of information at the right time and make full use of it. All types of industries, manufacturing, service, tertiary industries, all are dependent on computers and IT. It is impossible for an individual as well as for an organization to not use computers in today's age and continue to work. The use of computers and IT has increased the speed of working. It has ensured a hike in the efficiency levels. More importantly, it has been able to save time by the use of multi-tasking machines and gadgets. But there is a negative aspect of this. Due to more usage of computers and IT, the volume of cyber security threats has also shoot up very high. This risk is particularly higher in the developed nations because of the high use of computers in almost all activities. Prior researches have been done on the same topic or related topics.

A review of these literatures is added to the study to get an idea of these prior researches, the research methodology followed by those scholars, the conclusions reached by them and scope of research existing in that domain despite some prior researches pursued. Arsac, Wihem & Compagna, Luca & Pellegrino, Giancarlo & Ponta, Serena. (2011). More and more industrial activities are captured through Business Processes (BPs). To evaluate whether a BP under-design enjoys certain security desiderata is hardly manageable by business analysts without tool support, as the BP runtime environment is highly dynamic (e.g., task delegation). Automated reasoning techniques such as model checking can provide the required level of assurance but suffer of well-known obstacles for the adoption in industrial systems, e.g. they require a strong logical and mathematical background. In this paper, we present a novel security validation approach for BPs that employs state-of-the-art model checking techniques for evaluating security-relevant aspects of BPs in dynamic environments and offers accessible user interfaces and apprehensive feedback for business analysts so to be suitable for industry.J. Barnett, Daniel & Sell, Tara & Lord, Robert & J. Jenkins, Curtis & W. Terbush, James & Burke, Thomas. (2013). Ever-increasing threats to cyber security present serious challenges for population health. However, the direct intersections between cyber security and public health can benefit from examination through the lenses of public health system operational frameworks. In this paper, we thus provide an overview of how cyber security issues may systemically impact public health emergency preparedness and imperil the delivery of essential public health services. We discuss future broad-based policy and research considerations accordingly for this critical public health security dimension.

Ramadan, Qusai & Mohd, Masnizah. (2011). Retrospective news event detection (RED) has been studied for many years in order to discover previous unidentified events. There are ongoing works done to improve RED techniques such as distance measure and clustering approaches to overcome issues such as huge dimensionality of data. This paper discusses three major sequential stages in RED (data pre-processing, data representation and data organization) and reports the limitation in each stage. Finally we present the suggested RED with respect to crimes domain. Saleem, M.Q. & Jaafar, Jafreezal & Hassan, Mohd Fadzil. (2012). Business process modelling is very crucial for enterprises because it give an idea how the business would be operated in the real world and it is important for every stakeholder. SOA is one of the most popular architecture for building Web Information Systems. In current SOA system development practices, security is not defined at the early phases of software development and left on the developer. Properly configuring security requirements in SOA applications is quite difficult for developers because they are not security experts, furthermore SOA security is cross-domain and all required information are not available at downstream phases. The post-hoc, low-level integration of security has a negative impact on resulting SOA applications. Business process modelling is normally performed by the Business Process expert who is not a security expert. Furthermore current business process modelling languages like UML or BPMN do not support the specification of security requirements along the business process modelling. We have presented a DSL, to model the security requirements along the business process model. We are facilitating the Business Process expert to model the security in business process diagram. This security annotated business process model will facilitate the security expert in specifying concrete security implementation. As a proof of work the proposed DSL is applied to the modelling of a typical business process of "on-line student information system". Merat, Soorena & Almuhtadi, Wahab. (2015). the main focus of this paper is the improvement of machine learning where a number of different types of computer processes can be mapped in multitasking environment. A software mapping and modelling paradigm named SHOWAN is developed to learn and characterize the cyber awareness behaviour of a computer process against multiple concurrent threads. The examined process starts to outperform, and tended to manage numerous tasks poorly, but it gradually learned to acquire and control tasks, in the context of anomaly detection. Finally, SHOWAN plots the abnormal activities of manually projected task and compare with loading trends of other tasks within the group.

Modern information systems are large-sized and comprise multiple heterogeneous and autonomous components. Autonomy enables decentralization, but it also implies that components providers are free to change, retire, or introduce new components. This is a threat to security, and calls for a continuous verification process to ensure compliance with security policies. Existing verification frameworks either have limited expressiveness—thereby inhibiting the specification of real-world requirements—, or rely on formal languages that are hardly employable for modelling and verifying large systems. In this paper, we overcome the limitations of existing approaches by proposing a framework that enables: (1) specifying information systems in SecBPMN, a security-oriented extension of BPMN; (2) expressing security policies through SecBPMN-Q, a query language for representing security policies; and (3) verifying SecBPMN-Q against SecBPMN specifications via an implemented query engine. We report on the applicability of our approach via a case study about air traffic management. Salnitri, Mattia & Dalpiaz, Fabiano & Giorgini, Paolo. (2014) Modern information systems are large-sized and comprise multiple heterogeneous and autonomous components. Autonomy enables decentralization, but it also implies that components providers are free to change, retire, or introduce new components. This is a threat to security, and calls for a continuous verification process to ensure compliance with security policies. Existing verification frameworks either have limited expressiveness—thereby inhibiting the specification of real-world requirements—, or rely on formal languages that are hardly employable for modelling and verifying large systems. In this paper, we overcome the limitations of existing approaches by proposing a framework that enables: (1) specifying information systems in SecBPMN, a security-oriented extension of BPMN; (2) expressing security policies through SecBPMN-Q, a query language for representing security policies; and (3) verifying SecBPMN-Q against SecBPMN specifications via an implemented query engine. We report on the applicability of our approach via a case study about air traffic management.

Williams, T. (2007). The Canadian federal government plans to roll out a national strategy to protect critical infrastructure systems such as oil and gas pipelines, refineries, power plants, etc. from attacks either by hackers or terrorists. A discussion covers the Supervisory Control and Data Acquisition systems that monitor and control pipelines connect field sites to the control center; simple denial-of-service attack on the leak-detection system in a liquids pipeline; a combined attack that blends cyber and physical attack; internet exposure; and what to do during cyber-security incidents.

Mohammadi, Nazila & Heisel, M. (2017). The trustworthiness of systems that support complex collaborative business processes is an emergent property. In order to address users' trust concerns, trustworthiness requirements of software systems must be elicited and satisfied. The aim of this paper is to address the gap that exists between end-users' trust concerns and the lack of implementation of proper trustworthiness requirements. New technologies like cloud computing bring new capabilities for hosting and offering complex collaborative business operations. However, these advances might bring undesirable side effects, e.g., introducing new vulnerabilities and threats caused by collaboration and data exchange over the Internet. Hence, users become more concerned about trust. Trust is subjective; trustworthiness requirements for addressing trust concerns are difficult to elicit, especially if there are different parties involved in the business process. We propose a user-cantered trustworthiness requirement analysis and modelling framework. We integrate the subjective trust concerns into goal models and embed them into business process models as objective trustworthiness requirements. Business process model and notation is extended to enable modelling trustworthiness requirements. This paper focuses on the challenges of elicitation, refinement and modelling trustworthiness requirements. An application example from the healthcare domain is used to demonstrate our approach.

Mohammadi, Nazila & Heisel, M. (2017). The trustworthiness of systems that support complex collaborative business processes is an emergent property. In order to address users' trust concerns, trustworthiness requirements of software systems must be elicited and satisfied. The aim of this paper is to address the gap that exists between end-users' trust concerns and the lack of implementation of proper trustworthiness requirements. New technologies like cloud computing bring new capabilities for hosting and offering complex collaborative business operations. However, these advances might bring undesirable side effects, e.g., introducing new vulnerabilities and threats caused by

collaboration and data exchange over the Internet. Hence, users become more concerned about trust. Trust is subjective; trustworthiness requirements for addressing trust concerns are difficult to elicit, especially if there are different parties involved in the business process. We propose a user-cantered trustworthiness requirement analysis and modelling framework. We integrate the subjective trust concerns into goal models and embed them into business process models as objective trustworthiness requirements. Business process model and notation is extended to enable modelling trustworthiness requirements. This paper focuses on the challenges of elicitation, refinement and modelling trustworthiness requirements. An application example from the healthcare domain is used to demonstrate our approach. Maines, Curtis & Zhou, Bo & Tang, Stephen & Shi, Qi. (2016). Every so often a paper is published presenting a new extension for modelling cyber security requirements in Business Process Model and Notation (BPMN). The frequent production of new extensions by experts belies the need for a richer and more usable representation of security requirements in BPMN processes. In this paper, we present our work considering an analysis of existing extensions and identify the notational issues present within each of them. We discuss how there is as yet no single extension which represents a comprehensive range of cyber security concepts. Zhou, Bo & Maines, Curtis & Tang, Stephen & Shi, Qi & Yang, Po & Qi, Jun. (2018) Social Internet-of-Things (SIoT) environment comprises not only smart devices but also the humans who interact with these IoT devices. The benefits of such system are overshadowed due to the cyber security issues. A novel approach is required to understand the security implication under such a dynamic environment while taking both the social and technical aspects into consideration. This paper addressed such challenges and proposed a 3-D security modelling platform that can capture and model the security requirements in the SIoT environment. The modelling process is graphical notation based and works as a security extension to the Business Process Model and Notation. Still, it utilizes the latest 3-D game technology; thus, the security extensions are generated through the third dimension. Consequently, the introduction of security extensions will not increase the complexity of the original SIoT scenario, while keeping all the key information on the same platform. Together with the proposed security ontology, these comprehensive security notations created a unique platform that aims at addressing the ever complicated security issues in the SIoT environment.

Bhandayker, Yeshwanth. (2016). With thousands of thousands of brand-new hazards being exposed each day, it is additionally coming to be an increasing number of tough to continually turn out current endpoint security. Also if a security supplier had unlimited human capability to by hand examine as well as compose policies to shield versus every brand-new hazard found daily, the regularity, as well as dimension of the updates being presented to every endpoint service, would certainly be illogical, successfully damaging the online experience for the large bulk of clients. As a result, a mixed strategy, making use of a neighbourhood scanning engine in a mix with a cloud security engine, both powered by AI/ Machine Learning as well as big data is, our company believe, the maximum technique to supplying the most effective malware security. This paper has numerous research study studies on exactly how machine learning, as well as AI, can aid boost the security of computer system systems. Barcelo, Juan. (2018). “Artificial” intelligence is not just a discourse about robots. It is about understanding the nature of cognition using computers as experimental devices. Therefore, it deals with the nature of inferential mechanisms, and the particular way computer programs allow us to produce inferences. Computer scientists are exploring this subject and there are many algorithms and programs for knowledge expansion through iterative and recursive revision. Artificial intelligence offers us methods and techniques to explain archaeological data. Although statistical reasoning is still giving its support to all these methods, it is not classical statistical inference. Artificial intelligence paradigms differ from usual classification and clustering methods, in that they: (1) are robust in the presence of noise; (2) are flexible as to the statistical types that can be combined; (3) are able to work with feature (attribute) spaces of very high dimensionality; (4) can be based on nonlinear and nonmonotonic assumptions; (5) require less training data; and (6) make fewer prior assumptions about data distributions and model parameters.

REFERENCES:

1. Arpitha, kaustubh Dutta, "Impact of Machine Learning and Artificial Intelligence on Mankind",I2C2,2017.
2. Narendra kumar, Nidhi, Rashi," Ethical aspects and Future of AI",2016,ICICCS,111-114.
3. Arsac, Wihem & Compagna, Luca & Pellegrino, Giancarlo & Ponta, Serena. (2011). Security Validation of Business Processes via Model-Checking. 29-42. 10.1007/978-3-642-19125-1_3.
4. Arlindo Oliveria," Cyber Security and role of Artificial Intelligence".
5. Barcelo, Juan. (2018). Artificial Intelligence. 1-6. 10.1002/9781119188230.saseas0044.
6. B H, Rashmi. (2018). Impact of Artificial Intelligence on Cyber Security. International Journal of Computer Sciences and Engineering. 6. 341-343. 10.26438/ijcse/v6i12.341343.
7. Bhandayker, Yeshwanth. (2016). Artificial Intelligence and Big Data for Computer Cyber Security Systems. 12. 324-329.
8. Demertzis, Konstantinos & Liadis, Lazaros. (2018). Artificial Intelligence System for Cyber Security. 10.13140/RG.2.2.17090.07363.
9. Dr. Sunil Bhutada, Preethi Butada," Applications of AI in CyberSecurity", IJERCSE, Volume 5, Issue 4,214-219.
10. J. Barnett, Daniel & Sell, Tara & Lord, Robert & J. Jenkins, Curtis & W. Terbush, James & Burke, Thomas. (2013). Cyber Security Threats to Public Health. World Medical & Health Policy. 5. 10.1002/wmh3.19.
11. L. Maines, Curtis & Zhou, Bo & Tang, Stephen & Shi, Qi. (2016). Adding a Third Dimension to BPMN as a Means of Representing Cyber Security Requirements. 105-110. 10.1109/DeSE.2016.69.
12. Li, Jian-hua. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering. 19. 1462-1474. 10.1631/FITEE.1800573.
13. Mohammadi, Nazila & Heisel, M. (2017). A Framework for Systematic Refinement of Trustworthiness Requirements. Information (Switzerland). 8. 10.3390/info8020046.
14. Ogaba Oche, Joseph. (2019). The Risk of Artificial Intelligence in Cyber Security and the Role of Humans. TEXILA INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH. 1-7. 10.21522/TIJAR.2014.SE.19.01.Art001.
15. Maines, Curtis & Llewellyn-Jones, David & Tang, Stephen & Zhou, Bo. (2015). A Cyber Security Ontology for BPMN-Security Extensions. 1756-1763. 10.1109/CIT/IUCC/DASC/PICOM.2015.265.
16. Merat, Soorena & Almuhtadi, Wahab. (2015). Artificial intelligence application for improving cyber-security acquirement. Canadian Conference on Electrical and Computer Engineering. 2015. 1445-1450. 10.1109/CCECE.2015.7129493.
17. P. Santra,"An Expert Forensic Investigation System for Detecting Malicious Attacks and Identifying Attackers in Cloud Environment" Research Paper | Journal (IJSRNSC) Vol.6, Issue.5, pp.1-26, Oct-2018.
18. Ramadan, Qusai & Mohd, Masnizah. (2011). A review of retrospective news event detection. 2011 International Conference on Semantic Technology and Information Retrieval, STAIR 2011. 209-214. 10.1109/STAIR.2011.5995790.
19. Saleem, M.Q. & Jaafar, Jafreezal & Hassan, Mohd Fadzil. (2012). A Domain-Specific Language for Modelling Security Objectives in a Business Process Models of SOA Applications. INTERNATIONAL JOURNAL ON Advances in Information Sciences and Service Sciences. 4. 10.4156/aiss.vol4.issue1.45.
20. Thakur, Kutub & Tao, Lixin & Wang, Tianyu & Liakat Ali, Md. (2017). Cloud Computing and its Security Issues. Application and Theory of Computer Technology. 2. 1-10. 10.22496/atct20161210.
21. Williams, T. (2007). Cyber security threats to pipelines and refineries. 234. 56, 58.
22. Zhou, Bo & Maines, Curtis & Tang, Stephen & Shi, Qi & Yang, Po & Qi, Jun. (2018). A 3-D Security Modeling Platform for Social IoT Environments. IEEE Transactions on Computational Social Systems. PP. 10.1109/TCSS.2018.2878921.
23. W. Streilein, William & Dillman, Brad. (2018). Proceedings of the Artificial Intelligence for Cyber Security (AICS) Workshop 2019. This volume represents the proceedings of the Artificial Intelligence for Cyber Security (AICS) Workshop 2019, held on January 27, 2019 in Honolulu, Hawaii.