Capability Management in Resilient ICT Supply Chain Ecosystems

Jānis Grabis[1], Janis Stirna[2] and Jelena Zdravkovic[2]
[1]*Department of Management Information Technology, Riga Technical University, Kalku 1, Riga, Latvia*
[2]*Department of Computer and Systems Sciences, Stockholm University, Borgarfjordsgatan 12, Stockholm, Sweden*

Keywords: ICT Supply Chain, Capability, Digital Twin.

Abstract: An ICT system consists of multiple interrelated software and hardware components as well as related services. They are often produced by a complex network of suppliers the control of which is hard, time consuming and in many cases almost impossible for a single company. Hence, it is a common practice for malicious actors to target the ICT product supply chain assuming that some members have lax security practices or lag behind in terms of using the latest solutions and protocols. A single company cannot assure the security of complex ICT systems and cannot evaluate risks and therefore, to be successful it needs to tap into a wider network of ICT product developers and suppliers, which in essence leads to forming an ecosystem. We propose in this study that such an ecosystem should be established and managed on the bases of its members capabilities, which in this means capacity to meet desired goals, i.e., security and privacy requirements in a dynamic business context. The proposal is illustrated on the case of the ICT product called IoTool, which is a lightweight IoT gateway. The IoTool uses various third-party components such as sensors and actuators supplied by different vendors.

1 INTRODUCTION

An **ICT system** consists of multiple interrelated software and hardware components as well as related services. These services are often produced by a complex network of suppliers the control of which is hard, time consuming and in many cases almost impossible for a single company. Hence, it is a common practice for malicious actors to target the ICT product **supply chain** assuming that some of its members have lax security practices or lag behind in terms of using the latest solutions and protocols. From the perspective of a product developer, onboarding of new supply chain members is challenging, especially in the case of decentralized supply chains and short life-cycle products. Ongoing research suggests that many procurement professionals do not consider vendors' cybersecurity capabilities to be an important factor in selecting top-tier suppliers and calls for action to address this (Rogers and Choi 2018). There are many examples of supply-chain-induced vulnerabilities. For example, 40 million Target credit card data were stolen by exploring a security shortcoming in HVAC devices used at the stores and supplied by an external vendor or 40,000 U.K. users were affected by a data leak in a third party customer chat-bot (Kshetri and Voas 2019). Experts predict that these problems will be amplified by a rush for creating new devices and services relying on the 5G mobile network (Madnick, 2019) which would open the doors for malicious actors to exploit vulnerabilities.

The position of this paper is that any member of the ICT supply chain should have a **capability** to be able to contribute to the development of secure and trusted ICT systems (Zdravkovic et al., 2017). In this regard capability is seen as *an ability and capacity to meet desired goals (i.e., security and privacy requirements) in dynamic context* (Sandkuhl and Stirna, 2018).

A single company cannot assure the security of complex ICT systems and cannot evaluate risks. Therefore, the company needs to tap into a wider network of ICT product developers and suppliers, which leads to forming an **ecosystem.** *Being a part of a business ecosystem, provides a company with abilities to leverage its technology, achieve excellence in competences, as well as to collaborate and compete with other companies of various sizes*. Making a company and its business offerings to fit to a business ecosystem requires adjusting its goals, capabilities and processes, which also leads to improving the management of operations critical to success. An ecosystem is seen as a network of

Grabis, J., Stirna, J. and Zdravkovic, J.
Capability Management in Resilient ICT Supply Chain Ecosystems.
DOI: 10.5220/0009573603930400
In *Proceedings of the 22nd International Conference on Enterprise Information Systems (ICEIS 2020) - Volume 2*, pages 393-400
ISBN: 978-989-758-423-7

organizations bound by both cooperation and competition in their effort of delivering products and services. Since today's development and delivery of ICT products and services is carried out digitally, in this paper we are referring to **Digital Business Ecosystems (DBE).** Members of such an ecosystem have a joint interest to identify security threats and to establish trust, while they might have vastly different motivations in business terms. From the point of view of an ecosystem, a key security related motivator is the ability to ensure **trust and resilience**.

Evaluation of security concerns is an ongoing activity as ICT product supply chain topology continuously evolves in the dynamic context. A **data-driven digital twin** resembling the ICT product supply chain is used for continuous exploration and prediction of arising threats. The digital twin explores input and output data and limited knowledge of ICT product supply chain's internal structure to evaluate threats. The evaluation and enactment of mitigation actions require members' collaboration across the ecosystem. Hence, there is a need to develop *methods and business models* for enabling this collaboration and automated knowledge creation and application of mitigation solutions. The knowledge in turn will facilitate further design and auditing of ICT products and their supply chains.

As a step towards the elaboration of such a digital business ecosystem, the goal of this paper is *to conceptually outline a* ***method framework*** *and* ***an architecture of a software platform*** *for efficient development and management of* ***resilient*** *ICT supply chains in dynamically evolving ICT product* ***ecosystems.*** The proposed approach employs the principles of capability management and uses data-driven digital twins for collaborative security and trust evaluation.

The rest of the paper is structured as follows: Section 2 outlines our ecosystem-based approach for managing secure supply chains. Section 3 elaborates the digital twin component, focal for enabling security analysis in the chain. In section 4 a business case is described as a proof-of-concept. A discussion is given in section 5 including concluding remarks and future work.

2 THE DBE-BASED APPROACH

ICT product Supply chains deal with creating specific products or services, hence its ecosystem encompasses different supply chain members and other relevant business parties. The lead supply chain member creates an ICT product supply chain topology and the rest supply chain members (partners) are selected according to their ability to deliver trusted product capabilities.

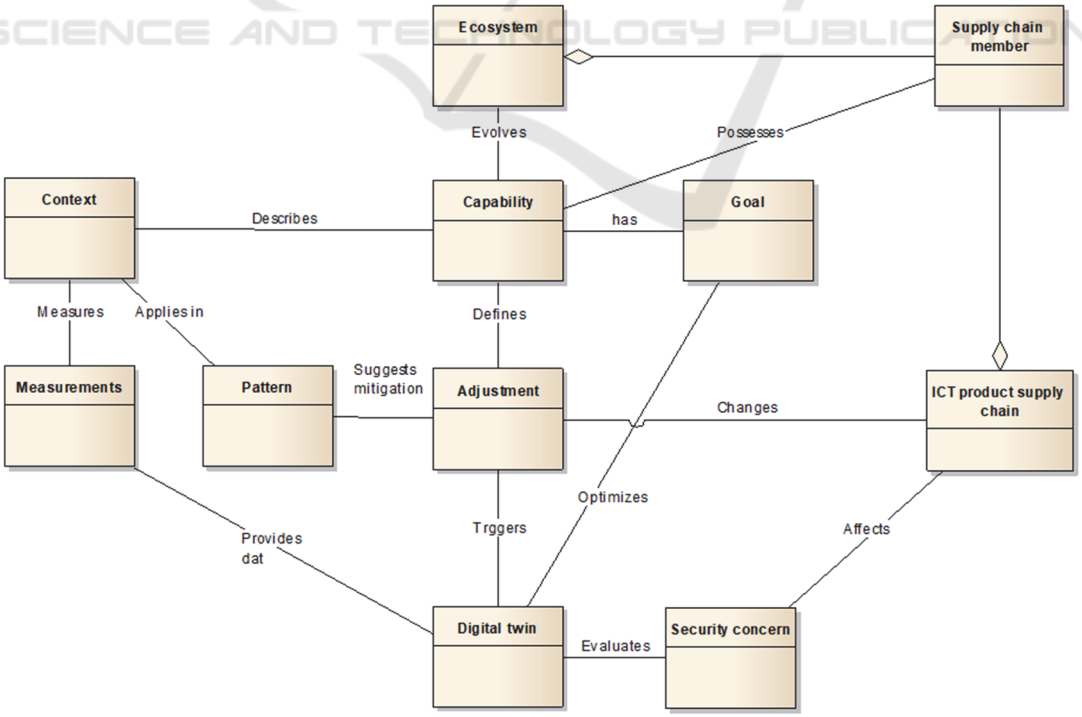

Figure 1: Conceptual model of the approach.

Our approach is based on the principle of a functioning and evolving Digital Business Ecosystem. It consists of the following core building blocks (1) the principle of ecosystems of supply chains for ICT systems for collaboration in terms of sharing knowledge for solving threats and building trust, (2) the notion of capability for configuring the supply chains with goal and context awareness, (3) the need to develop and manage digital twins to simulate and predict the behaviour of the supply chain from the data of executing capabilities, and (4) a collaboration-based approach to the reconfiguration and adjustment of supply chains to ensure needed security and optimal trust. In Figure 1 the core conceptualisation for our DBE-based approach is presented:

Capability defines a supply chain's member's ability to provide secure and trusted products and services. It serves as a protector for selecting *supply chain members*, which are required to share common *goals*, provide required *contextual information*, as well as to share knowledge to a degree of trust required in the supply chain. The elements of a capability externally relevant are exposed through its interface visible to any supply chain member being involved in the ecosystem. Any context data of any capability of the members is captured by *measurable properties* (event logs, sensors) and streamed to the *digital twin* of the supply chain. The twin is responsible to detect any adverse *security concern* related event, including trust and privacy violations from the data received; it then acts, by relying on the *knowledge patterns* available in the ecosystem, and determine *adjustments* of related capabilities to stop or diminish undesired behaviour measured by capability's KPI.

The capabilities are continuously developed in the ecosystem by accumulating and formalizing secure ICT product supply chain management knowledge (Figure 2). The ICT product supply chain is dynamic with hidden tiers, members, and connections, and live supply chain and context data are analysed to uncover these hidden aspects. A data-driven digital twin is created to explore various supply chain operations scenarios and for predicting the need for appropriate adjustments. As the result, the supply chain topology is updated. The topology reflects not only elements defined in the initial design but also ones discovered during supply chain operations.

Live ICT product supply chain analysis and experimentation lead to knowledge discovery, i.e. to eliciting the information relevant for dealing with security concerns; which contextual information is needed; and which data trends indicate security threats. The knowledge is represented using patterns that are subjected to collaborative evaluation in the ecosystem. The patterns accepted by the chain community contribute to further development for secure supply chain management capabilities.

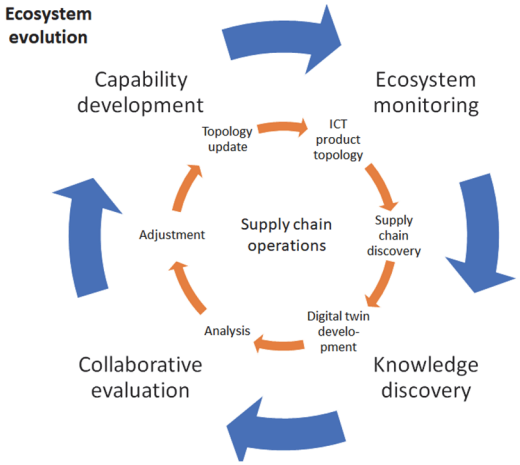

Figure 2: Dynamic interactions in the ICT product supply chain and ecosystem.

3 DATA-DRIVEN DIGITAL TWIN

A data-driven digital twin is a digital representation of an ICT product supply chain on the basis of live data streams for the purposes of analysis of security concerns and experimentation (Figure 3). The ICT product supply chain is only partially observable and there is some level of uncertainty and missing data in its representation. Therefore, it is referred as to data-driven because of relaxed requirements in terms of knowing the internal structure of the supply chain. The digital twin receives data about a live ICT product supply chain as specified in the Model representing capabilities of the suppliers. *The data are representing the product and supply chain perspectives*. The data streams are analysed to identify irregularities and to benchmark them against the normal behaviour captured in the patterns. The digital twin itself is used to predict the behaviour of the ICT product supply chain and to propose adjustments to cope with security concerns and to reconfigure the supply chain. The digital twin uses a learning based prediction model. The Design-of-experiments (DOE) module is used to specify manually or automatically scenarios to be explored to identify weaknesses and potential threats. The Simulator module is responsible for generating the scenarios. The evaluation scenarios are visualized and the prediction results are transferred to the portal and the dashboard.

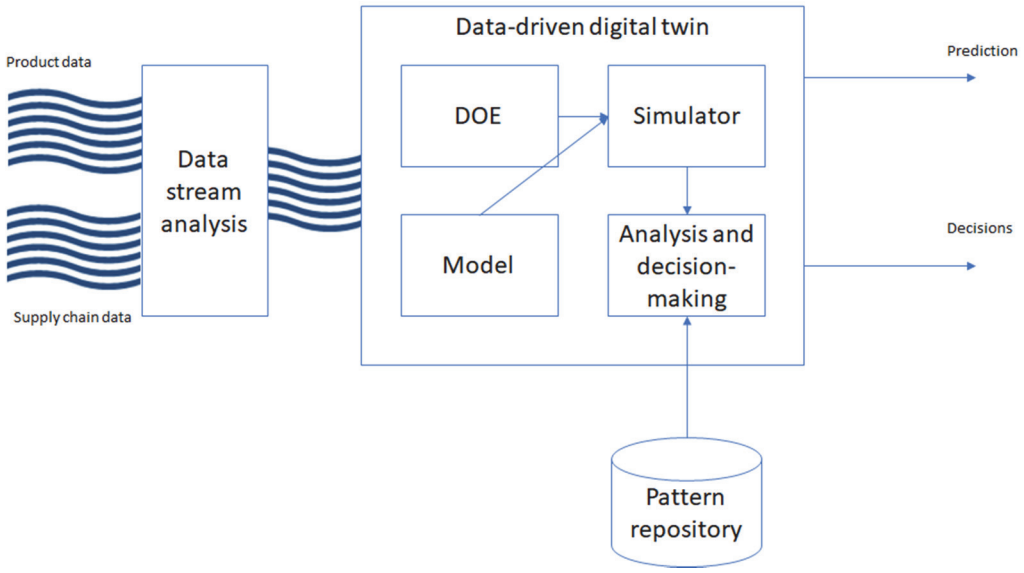

Figure 3: Components of the data driven digital twin.

4 PROOF-OF-CONCEPT

The example case considers an ICT product called IoTool[1], which is a lightweight IoT gateway. The IoTool uses various third-party components such as sensors and actuators supplied by different vendors. The tool vendor needs to ensure that the components are trusted, i.e. that they do not compromise IoTool end-users. Currently, the IoTool design implements fair-enough security, but it needs to face the interoperation with additional untrustworthy IoT devices and protocols which usually are black-boxes in the sense that offer little information with regard to which security and privacy protections they implement.

4.1 Capability Model

The IoTool solution uses some out-of-the-box devices (e.g. smartphones) which are not 100% secure; as well as the final users want to use them for other purposes (e.g. as personal devices). It is necessary therefore to ensure that the data transport protocol is secured to keep data integrity and confidentiality. By adopting the envisioned DBE-based approach, the IoTool requires that vendors of the connected devices provide the secure-sensing capability (Figure 4). The goals of secure-sensing capability are to preserve data privacy and to prevent using sensing devices for DOS or similar malicious activities as well as to have an appropriate risk level and to provide the desired features requested from customers. To ensure that the ICT product supply chain is able to achieve these goals, the context is defined, where the vendors and devices are characterized by their trustworthiness and vulnerabilities. Measurable properties (i.e., raw data) are used to evaluate the context. Both internal and external data sources are used.

The ICT product supply chain topology including its product design and supply chain configuration is developed (Figure 5). There is a choice between various providers, for example, the IoTool can use different cloud storage vendors, which could be also selected according to their ability to support the secure-sensing capability. Once the IT environment supporting the digital twin for the supply chain is put in place, the context is continuously evaluated on the basis of the measurable property data and if irregularities are observed the supply chain is reconfigured. For example, in case external data sources provide a report that one of the vendors has supplied insecure devices and the Vendor trustworthiness falls below a certain threshold set by the IoTool vendor, the sensors provided by this supplier are excluded from the offering.

[1] https://iotool.io/

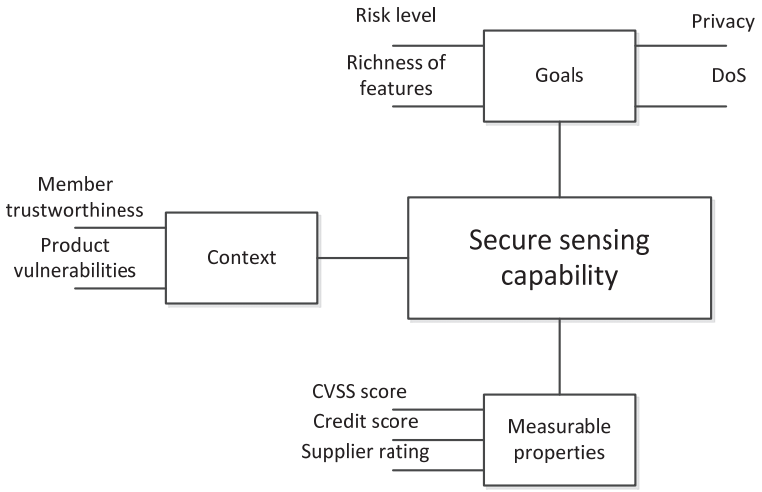

Figure 4: Secure sensing capability model.

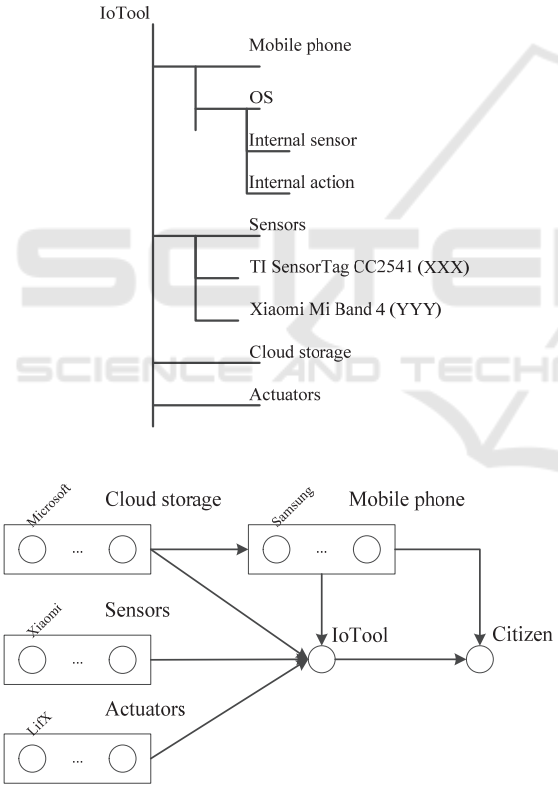

Figure 5: Fragments of IoTool product design and supply chain. The rectangles represent products; circles represent vendors or supply chain members.

4.2 Supply Chain Configuration

ICT supply chain is continuously monitored for security concerns. The digital twin employs various models to represent and to analyse the supply chain. A data driven supply chain configuration model (Grabis et al. 2012) is one of these models. It uses the current data to evaluate agreement of the established supply chain typology with goals defined in the capability. In the sample model provided, the supply chain risk minimization is considered. The model selects supply chain members (referenced using index j) and products (references using index i) to minimize the overall supply chain level of risk R (Eq. 1). The risk is calculated by taking into account the context factors, namely, the product vulnerability score a_i and supply chain member trustworthiness score b_j. The parameters w_i indicate the relative importance of the product item in the ICT product and γ_{ij} is 1 if the ith product is provided by the jth supply chain member and 0 otherwise. The decision variable X_{ij} is 1 if the ith product provided by the jth supply chain member is included in the ICT product supply chain and 0 otherwise.

$$R = \sum_{i=1}^{M} \sum_{j=1}^{N} w_i a_i b_j \gamma_{ij} X_{ij} \rightarrow \min \quad (1)$$

Eq. 2 requires the minimum set of features for the ICT product stating that a function f of the selected products should be larger than a specified threshold F.

$$f(\mathbf{X}) \geq F \quad (2)$$

Moreover, any selected supply chain member is required to possess the secure sensing capability what is represented by constraints in Eq. 3-5. The overall trustworthiness risk contribution for any supplier should not exceed the threshold T (Eq. 3). The product item individual risk contribution should not exceed the threshold U (Eq. 4). The supply chain member trustworthiness score should be available

(Eq. 5), i.e. context data about the member should be available.

$$\sum_{i=1}^{M} w_i b_j \gamma_{ij} X_{ij} \leq T, \forall j \quad (3)$$

$$a_i b_j \gamma_{ij} X_{ij} \leq U, \forall i, j \quad (4)$$

$$b_j \neg \varnothing, \forall j \quad (5)$$

The ICT supply chain monitoring and configuration results are represented using a dashboard (Figure 6.) The dashboard shows the current overall risk, the trustworthiness of individual supply chain members and the vulnerability dynamics of the product items. It is assumed that the trustworthiness score is evaluated using data (i.e., measurable properties) provided from a credit scoring agency (e.g., https://www.companyhouse.de/) and the product vulnerability score is evaluated using data from the Common Vulnerabilities and Exposures database (https://cve.mitre.org/).

The example shows that the overall risk is below the required threshold, however, the trustworthiness of one of the supply chain members has declined. Therefore, a supply chain configuration model execution round should be triggered and recommendations for supply chain reconfiguration should be generated.

5 RELATED WORK

ICT products are ubiquitous and of major importance in businesses and societies. These products are highly modular and their components are sourced globally. However, they often lack transparency and their design evolves rapidly. Therefore, the supply chain perspective of ICT products grows rapidly (Lu et al., 2013). The concurrent product-supply chain design is widely accepted in the supply chain management theory and practice (Gran and Grunow, 2016). However, the traditional supply chain configuration methods (Chandra and Grabis, 2016) are not suitable for secure ICT product supply chains because supply chain topology is highly complex and rapidly evolving. Traditional supplier on-boarding and quality assurance techniques (Nikou et al., 2017) are too time-consuming and require detailed product design information. Data analytics help to uncover complex supply chain topologies (Zhao et al., 2018), though currently, the analysis is based on static data structures. There are a number of developments on secure supply chain management (Hasan et al., 2020) as well as security concerns specifically from the ICT perspective (Polatidis et al., 2017). However, these methods are based on traditional security management frameworks as well as they rely on static analysis and periodic product and process inspection.

Lately, the principle of the DBE has received attention for supporting and analysing networks of companies and collaboration among them, cf., for instance, (Conti et al., 2019; de Reuver et al., 2018; Mäntymäki et al., 2018; Senyo et al,. 2017). The state of the art in this area is mostly devoted to discussion the viability of the ecosystem-based approach and to proposing theoretical foundations.

Capability management (Sandkuhl and Stirna, 2018) is an approach to maintain viable DBEs. It brings together organizations by sharing common value, information and knowledge what can be successfully applied also for security management purposes. Lately, capability management has been extended by open data processing for the purpose of ensuring that business capabilities can be adjusted

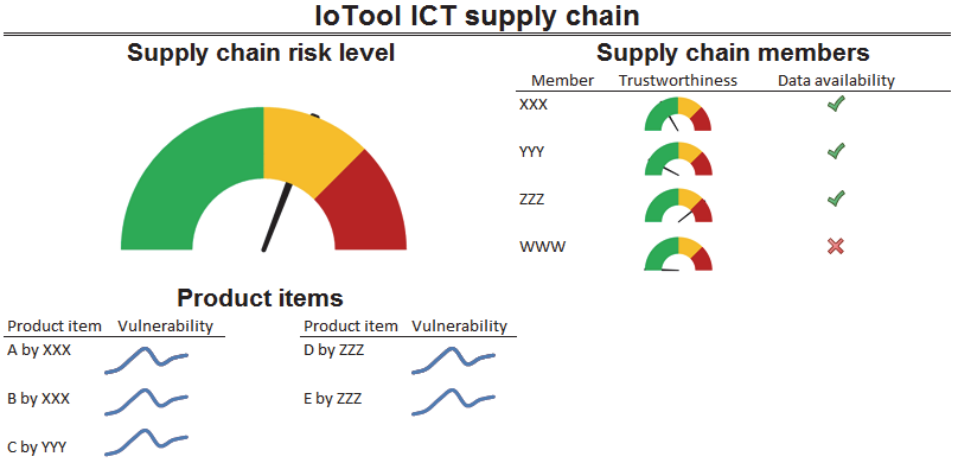

Figure 6: Sample ICT supply chain dashboard.

and configured dynamically at run-time (Kampars et al., 2019). Data stream processing is used to analyse data needed for capability development and analytical tools like digital twins can be used to evaluate the required adjustment.

In the best and most advanced cases (Kritzinger et al., 2018) digital models of supply chains are created automatically (by analysing large sets of data available in the existing ERP systems), which allows speaking of digital shadows. These models are called "shadows" because they do not provide automatic mechanisms of intervention into the real world supply chains for solving emerging business changes, challenges, and disruptions. The proposal aims to create true digital twins that will be created automatically and provide means for automatic configuration of the supply chain of ICT products. The concept of digital twins just recently started to get attention for application in the security management domain. For instance, (Eckhart et al. 2019) propose to use digital twins to rise cyber situational awareness for cyber-physical systems through visualizations. Viability of using data streams in digital twining has been recently demonstrated by (Murphy et al. 2020).

6 DISCUSSION AND CONCLUSIONS

This paper has presented a method framework and an architecture of a software platform for efficient development and management of resilient ICT supply chains in dynamically evolving ICT product ecosystems. The proposed approach is based on capability management in digital business ecosystems and it uses data-driven digital twins for collaborative security and trust evaluation. The specific novel contributions of the envisioned approach are as follows. (1) A method bringing together separate and diverse methods and tools (capability management, digital twins, data stream processing) to provide users with evidence-based guidance to design and execute trusted and secure ICT product supply chains. (2) Model-driven ICT product supply chain optimization according to business concerns such as goals and qualification constraints. These are specified in the supply chain capability model to account for reconfiguration needs, supply chain partner selection, concurrent product design, as well as for the fulfilment of trust and security requirements. (3) The envisioned approach allows including AI-based data streaming solutions for graphs with changing structure, such as dynamic ICT product supply chain topology and variable data sources for identifying security concerns and for discovering supply chain management pain-points for further analysis using digital twins and security services. (4) Data-driven digital twin of combined physical and virtual entities with limited knowledge of internal structure of ICT product supply chain, for predicting the behaviour of the chain, proposing the adjustments for coping with identified security problems, and for reconfiguring the supply chain. (5) Evidence-based collaborative evaluation of security concerns using specialized security management services and pattern discovery that allow sharing supply chain knowledge to relevant collaboration partners on mutually beneficial terms.

REFERENCES

Chandra, C., Grabis, J., 2016. *Supply Chain Configuration*, *Springer*.

Conti, V., Ruffo, S.S., Vitabile, S. et al. 2019. BIAM: a new bio-inspired analysis methodology for digital ecosystems based on a scale-free architecture. *Soft Computing, Springer, pp 1133–1150.*

de Reuver, M., Sørensen, C., Basole, R. C., 2018. The Digital Platform: A Research Agenda. *Journal of Information Technology, 33(2), 124–135*.

Eckhart, M., Ekelhart, A., Weippl, E., 2019. Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins, *IEEE International Conference on Emerging Technologies and Factory Automation, 1222*.

Grabis, J., Chandra, C., and Kampars, J., 2012. Use of distributed data sources in facility location, *Computers and Industrial Engineering, vol. 63, no. 4, pp. 855-863*.

Gran, T., Grunow, M., 2016. Concurrent product and supply chain design: a literature review, an exploratory research framework and a process for modularity design, *International Journal of Computer Integrated Manufacturing, 29, 12, 1255-1271*.

Hasan, M.M., Jiang, D., Ullah, A.M.M.S. Noor-E-Alam, M., 2020. Resilient supplier selection in logistics 4.0 with heterogeneous information, *Expert Systems with Applications, vol. 139, 112799*.

Kampars, J., Grabis, J. 2017. Near Real-Time Big-Data Processing for Data Driven Applications. *Innovate-Data 2017: 35-42.*

Kampars, J., Zdravkovic, J., Stirna, J., and Grabis, J., 2019. Extending organizational capabilities with Open Data to support sustainable and dynamic business ecosystems. *International Journal of Software and Systems Modeling, 1-28*.

Kritzinger, W., Karner, M., Traar, G., Henjes, J. & Sihn, W., 2018. Digital Twin in manufacturing: A categorical literature review and classification, *IFAC-PapersOnLine, vol. 51, no. 11, pp. 1016-1022*.

Kshetri, N., Voas, J.M., 2019. Supply Chain Trust. *IT Professional 21(2): 6-10.*

Lu, T., Guo, X., Xu, B., Zhao, L., Peng, Y. & Yang, H., 2013. Next big thing in big data: The security of the ICT supply chain, Proceedings - SocialCom/PASSAT/ BigData/EconCom/BioMedCom 2013, pp. 1066.

Madnick, S., 2019. 5G security concerns persist with new research pointing to critical flaw, https://www.itpro.co.uk/mobile/32893/

Mäntymäki M., Salmela H., Turunen M., 2018. Do Business Ecosystems Differ from Other Business Networks? The Case of an Emerging Business Ecosystem for Digital Real-Estate and Facility Services. In: *Al-Sharhan S. et al. (eds) Challenges and Opportunities in the Digital Era. LNCS 11195, Springer*.

Murphy, A., Taylor, C., Acheson, C., Butterfield, J., Jin, Y., Higgins, P., Collins, R. & Higgins, C., 2020. Representing financial data streams in *digital simulations to support data flow design for a future Digital Twin, Robotics and Computer-Integrated Manufacturing, vol. 61*.

Nikou, C., Moschuris, S.J., Filiopoulos, I., 2017. An integrated model for supplier selection in the public procurement sector of defence, *International Review of Administrative Sciences, vol. 83, pp. 78-98*.

Polatidis, N., Pavlidis, M., Mouratidis, H., 2018. Cyber-attack path discovery in a dynamic supply chain maritime risk management system, *Computer Standards and Interfaces, vol. 56, pp. 74-82*.

Rogers, Z., Choi, T.Y., 2018. Purchasing Managers Have a Lead Role to Play in Cyber Defense, *Harvard Business Review*.

Sandkuhl, K., Stirna, J., 2018. Capability Thinking, in Capability Management in *Digital Enterprises, Springer*.

Senyo P.K., Liu, K., Effah, J., 2017. Towards a methodology for modelling interdependencies between partners in digital business ecosystems, *IEEE international conference on logistics, informatics*.

Zdravkovic, J., Stirna, J., Grabis, J., 2017. A Comparative Analysis of Using the Capability Notion for Congruent Business and Information Systems Engineering. *International Journal Complex Systems Informatics and Modeling Quarterly 10, pp 1–20*.

Zhao, K., Scheibe, K., Blackhurts, J., Kumar, A., 2018. Supply Chain Network Robustness Against Disruptions: Topological Analysis, Measurement, and Optimization. *IEEE Transactions on Engineering Management, 66, 1, 127–139*.