An Overview of Security Management in Supply Chain

Tomiloba Olutola [1], John Balen [1], Chidi Yun [1], Miki Shun [1] , Vivian Lotisa [2], Akaw Johnima [2], Ladson Newiduom [2], Ibrina Browndi [2]
[1] Department of Computer Science, Rivers State University, Port Harcourt, Nigeria
[2] Department of Urban and Regional Planning, Rivers State University, Port Harcourt, Nigeria

ABSTRACT

Supply Chain Security Management [SCSM] is a relatively new discipline in the field of Operations Management Research, thus lacking introductory and tutorial papers. The recent concerns on security in global supply chains are driving the introduction of new security initiatives, standards and measures to such an extent that they are becoming an integral part of supply chain management. This paper presents the current state of SCSM initiatives, and discusses their managerial implications, including the importance of interplay between various parties, i.e. authorities, manufacturers, distributors etc., to support the fluent and secure flow of goods in the global economy The paper concludes that a gap exists between theoretical supply chain security studies, emerging security standards and practical managerial actions, and that the academic research community has a clear mission to bridge this gap, e.g. via pragmatic case studies within real world supply chains.

KEYWORDS: Supply Chain Security Management, Supply Chain Security Programs, Supply Chain Security Standards

1.0 INTRODUCTION

Security, its demands and constraints, constitute obstacles (logical and physical barriers) in the flow of supply and distribution. These “barriers” created by a perceived increased need for security, or political reasons, reduce the reaction capacity and the physical and economical performance of the company. Integrating the security dimension into the logistics strategy, organization and operations has become a new challenge for supply chain management [1-17].

The recent security concerns have led to the development of multiple initiatives and potential solutions to enhance security in international supply chains without affecting efficiency. Businesses, governments and researchers are tackling the problem from different perspectives and by using several methodologies. However, inherent complexities such as the large quantity and diversity of the actors involved in international supply chain processes, and the need to identify cost-effective security measures, have generated multiple academic research questions in the domain of SCSM. Among others, the relevant research topics can include [18-26]:

- What government- and business-community driven SCSM programmes, regulations and standards have emerged since 9/11 and will emerge in the foreseeable future?

- Whatarethenewsecuritymeasuresandparadigmsthatcompaniesshouldimplement, and which will affect their existing SCSM practices?

- What are the real cost and operational impacts that SCSM programs, regulations and standards have on companies – from small- and medium-sized enterprises (SMEs) to Multinational Companies (MNCs), at various industrial and national levels?

- What are the broader topics surrounding SCSM initiatives and decisions, including global trade facilitation, technical trade barriers etc.?

This SCSM paper aims to present a pragmatic framework for future research, regulations development, and industry practitioner purposes, with the following three-step approach [27-40]:

- By providing an overview of SCSM background and evolution.
- By providing an overview of existing SCSM initiatives from governments, businesses, international organizations and researchers, and by working out a preliminary framework to classify them.
- By presenting possible impacts for business actors of international supply chains; and discussing the future views and predictions.

2.0 LITERATURE REVIEW

By SCSM, we mean enhancing and embedding the traditional security management aspects into holistic management of integrated supply chains, especially within a global context. SCSM has roots in multiple fields: Supply Chain Management; International Trade, Logistics and Cross-border Operations Management; Supply Chain Resilience Management; Quality Management; Risk Management; Insurance Policies and Instruments; and Customs Policies, Procedures and Reforms [1-11].

Since 2001 governments, Customs administrations, international organizations, researchers, and businesses have carried out diverse actions, and delivered different types of reports, and articles on the topic. The first pure SCSM paper was published at MIT, a few months after the infamous terrorist attacks in September 2001. Since then, researchers and industrial practitioners have organized and published SCSM conference and journal papers, primarily in the US but also in Europe and other continents [12-22].

Most of the researchers, presently contributing to building SCSM theory, have mainly been active in research fields such as Transportation and Logistics, Supply chain Management and Supply chain risk and vulnerability. The existing literature on SCSM, is somehow adding a layer of security to each researcher's own expertise domain. Some of the discussed principles are presented in the following paragraphs [23-39].

Projects present the need for companies to simultaneously operate under heightened security environments and the need to prepare for rapid recovery after terrorist attacks. In addition he establishes seven supply chain design trade-offs that management will face when designing secure supply chains: i) Repeatability vs. unpredictability ii) The lowest bidder vs. the known supplier. iii) Centralization vs. dispersion. iv) Managing risk vs. delivering value. v) Collaboration vs. secrecy. vii) Redundancy vs. efficiency and vii) Government cooperation vs. direct shareholder value [40-48].

Rice et al. (2003), presents the need for companies to simultaneously build secure and resilient supply chains. He identifies potential actions to improve physical, freight and information security, classifying them into four levels: Level 1 – Basic (i.e. physical security measures such as access control, badges, camera systems); Level 2 – Reactive (i.e. existence of supply continuity plans, analyse of supply bases); Level 3 – Proactive (i.e. Advanced cyber security, Business continuity plans); and Level 4 – Advanced (i.e. learning from past disruptions, formal security strategies) [44-51].

By SCSM, we mean enhancing and embedding the traditional security management aspects into holistic management of integrated supply chains, especially within a global context. SCSM has roots in multiple fields: Supply Chain Management; International Trade, Logistics and Cross-border Operations Management; Supply Chain Resilience Management; Quality Management; Risk Management; Insurance Policies and Instruments; and Customs Policies, Procedures and Reforms [1-13].

Since 2001 governments, Customs administrations, international organizations, researchers, and businesses have carried out diverse actions, and delivered different types of reports, and articles on the topic. The first pure SCSM paper was published at MIT, a few months after the infamous terrorist attacks in September 2001. Since then, researchers and industrial practitioners have organized and published SCSM conference and journal papers, primarily in the US but also in Europe and other continents [14-29].

Most of the researchers, presently contributing to building SCSM theory, have mainly been active in research fields such as Transportation and Logistics, Supply chain and Supply chain risk and vulnerability. The existing literature on SCSM, is somehow adding a layer of security to each researcher's own expertise domain. Some of the discussed principles are presented in the following paragraphs [30-38].

Project presents the need for companies to simultaneously operate under heightened security environments and the need to prepare for rapid recovery after terrorist attacks. In addition he establishes seven supply chain design trade-offs that management will face when designing secure supply chains: i) Repeatability vs. unpredictability ii) The lowest bidder vs. the known supplier. iii) Centralization vs. dispersion. iv) Managing risk vs. delivering value. v) Collaboration vs. secrecy. vii) Redundancy vs. efficiency and vii) Government cooperation vs. direct shareholder value [39-46].

Researcher presents the need for companies to simultaneously build secure and resilient supply chains. He identifies potential actions to improve physical, freight and information security, classifying them into four levels: Level 1 – Basic (i.e. physical security measures such as access control, badges, camera systems); Level 2 – Reactive (i.e. existence of supply continuity plans, analyse of supply bases); Level 3 – Proactive (i.e. Advanced cyber security, Business continuity plans); and Level 4 – Advanced (i.e. learning from past disruptions, formal security strategies) [47-51].

Projects draw lessons from total quality management programs applicable to the world of supply chain security management. Following the famous slogan from quality management, he argues that security is free; as long as it is assured with security measures that also increase supply chain efficiency [1-9].

Researchers argue that the challenge is to manage and mitigate supply chain risk by creating more resilient (flexible, agile) supply chains. They establish the four basic principles that support resilient supply chains: i) resilience should be designed in the processes. ii) There is a need for a high amount of collaboration iii) resiliency implies agility, which means being able to react quickly and iv) fostering a risk management culture within an organization is a prerequisite for resiliency [10-21].

Apart from researchers, governments and international organisations are currently very active in the design of supply chain security programs, regulations and standards, while businesses are settling for mandatory measures and participating in the design of some of these new measures. It could be argued that at the present time, the main challenge facing governmental actors is to define and implement adequate control measures which increase security without jeopardizing trade or burdening themselves and businesses with additional excessive operational costs. The main challenge for businesses is to invest wisely in security in such a way that they comply with the new regulations and at the same time achieve potential additional benefits that contribute to their supply chain efficiency [22-39].

The interaction between all these actors, shall define the future of SCSM as a new research discipline. It has yet to be determined whether academics will contribute to the development of security standards and policies or whether the new security regulations will constitute new restrictions to be tackled by the academic world. In addition the lack of academic papers mapping the research into practical actions in the real world is still a great chasm that has to be bridged [40-51].

3.0 RESEARCH METHODOLOGY

Multiple types of responses and actions have been undertaken by different governmental organisations, international organisations and businesses to enhance global supply chain security. These reactions range from country specific operational regulations to global research programs. They have different originating agents and they target specific goals. An extensive literature review, the multiple conference venues, discussion groups and security related events have allowed researchers to identify the most appropriate responses and actions in this field. It has been observed that most of these initiatives vary in the following ways:

- Type of originating actor: International organizations, governmental agencies (i.e. Customs administrations; Frontier guards; Border police; Transportation authorities; Home affairs offices, etc.), private sector.

- Transport mode (sea, air, road, rail)
- Enforceability: Mandatory vs. voluntary,
- Main specific goal: Enhancing Customs administrations security control capacity, reducing specific industry/geography vulnerability, developing global security standards, Technology development.

The following table presents an extensive list of the existing initiatives, organized by the category iv) described above, and by providing the value for the other dimensions presented.

Table 1. Classification of security initiatives by type of specific goal

Enhancing Customs Administrations security control capacity				
Action/ Response	Originating actors	Transport modes	Enforceability	Examples
Adding the security layer to existing Customs compliance programs	Governmental agencies	All	Voluntary	PIP (Canada), StairSec (Sweden), ACP & Frontline (Australia), AEO (EU)
Designing and implementing supply chain security programs	Governmental agencies	All	Voluntary	C-TPAT(USA), Secured Export Partnership (New Zealand)
Preventing at the source and using advance information	US government	Sea	Voluntary	CSI Container security initiative. US customs officers control cargo in foreign ports before they arrive at US borders.
		Sea	Mandatory	24 hour rule advance manifest rule and 96-hr notification of arrival vessel
Reducing specific industry/geography vulnerability				
Companies with high risk products or operating in risky regions designing security programs	Private sector	All	Voluntary	BASC (Latin America), against drug smuggling and TAPA (technology companies) against cargo theft.
Establishing specific regulations for risky transport modes	International Organisations	Sea	Mandatory	ISPS by IMO
		Air	Mandatory	Aviation security plan of action by ICAO
Developing global security standards				
Establish security standards that can be generalized for the entire Customs and trading community	International Organisations	All	Voluntary	WCO Framework of Standards to Secure and Facilitate Global Trade.
Become the leading supply chain security management standard.		All	Voluntary	ISO (International organization for standardization)
Technology development and deployment for security purposes				

Testing and evaluation of container scanning and tracking technology	Governmental agencies & private sector	Sea	Voluntary	OSC, Operation Safe Commerce.
Testing and evaluation of a complete tracking system along a secured trade lane	Private sector	All	Voluntary	SST, Smart and Secure Tradelane project.

Apparently there is a great variety of initiatives, all targeting supply chain security enhancement, but from different perspectives. However, a closer analysis of the concrete security measures promoted by each initiative showed that there are several areas in which they overlap or at least are interconnected. For instance, it was observed that the practical SCSM measures proposed by various initiatives typically fall into the following five intuitive categories:

Table 2. SCSM practical measures categories

Category	**Samples of practical security measures**
1. Cargo management: Protecting cargo during all steps of manufacturing, shipping and transport processes.	• Efficient prevention, detection and reporting of shipping process anomalies (routes and schedules continuous review; alerts management, etc.) • Adequate inspections during the shipping process (in points where liability changes, to packaging materials and vehicles before being in contact with cargo etc.).
2. Facility management: Guaranteeing the security of the facilities where goods are manufactured and cargo is stored and handled.	• Optimal warehouse/terminal layout design (entry/exit controllability; clearly marked control areas; sufficient light conditions etc.) • Efficient facility monitoring (24hr camera system, security guards, filming activities of loading containers, picking etc.).
3. Information management: Protecting critical business data and exploiting information as tool for detecting illegal activities and preventing security breaches.	• High protection of business information/data (management procedures and storing methods designed to protect information from unauthorized access and usage) • Accurate and complete recordkeeping of shipping information for potential security audits (improved recordkeeping methods; quality control of records, errors correction etc.).
4. Human resources management: Guaranteeing trustworthiness and security awareness of all personnel with physical or virtual access to the supply chains	• Professional employee hiring / exit process (background checks; interviews for leaving or fired employees etc.) • Efficient information dissemination process (internal and external publication of the company security policies).
5. Company management systems: "Building security" into internal and external organizational structures and company management systems, including supplier, partner and client management processes	• Adequate business partners evaluation system (selection of low risk and high security compliant suppliers, clients and subcontractors) • Complete company security management system (defined security processes, defined and controlled security indicators, internal and external audits, etc.)

4.0 RESULT

It was observed that Cargo management is emphasised by most of the prevailing security initiatives. Facility management and Human resources management are mainly mentioned in supply chain security programs created either to enhance Customs administrations security control capacity or to reduce specific industry/geography vulnerability. It was noted that practical measures falling into Information management category are a very important component of the efforts to enhance Customs administrations control capacity. For instance, the 24 hour advance manifest rule and 96-hr notification of vessel arrival are part of the few existing mandatory measures, and consist of managing the information flow on cargo in such a way that the risk can be detected before the physical flow arrives at the border. Finally, the fifth category provides the broadest view of SCSM.

Measures that fall into this category appear to be less straightforward to implement. There might be multiple potential good ways to implement them and different criteria to decide upon the required security level for a company, depending on its specific situation. In addition, it is highly probable that the implementation of these measures will require changes at strategic levels.

Apart from the actual SCSM measures, one should also consider the emerging SCSM (sub)-paradigms and their possible implications, such as:

- ‘Advance cargo information’ schemes refer to sending cargo- and trader-related Customs clearance and other data before goods arrive at certain points, i.e. border crossings or even pre-departure.
- ‘Known shipper’ and ‘authorised economic operator’ schemes mean identifying trustworthy companies which are given privileges in international supply chains.
- ‘Secure trade corridor’ schemes mean creating security controlled end-to-end transportation pipelines with state of the art tracking, screening and other capabilities, especially in the maritime environment.
- ‘Security built into products and processes’, and ‘integrated supply chain security management’ mean embedding security deep into the business, e.g. by following analogical approaches of total quality management while creating secure supply chains.

It can be argued that although there are common elements among many initiatives, each of them is nevertheless an independent effort to tackle different aspects of SCSM. Most of them are still in the developing stage and they will continue to suggest new operating processes and protocols, regulations and adoptions of new technologies. Whether or not these initiatives will converge is a new research question for the SCSM discipline. The authors of this paper believe more in opt for the “mutual recognition” between them, rather than in the establishment of a single global security standards system. There is a discrepancy between the development of security standards and the practical actions taken within companies worldwide – it would be beneficial to bridge the gap in the future, or at least oblige companies to take more actions.

5.0 DISCUSSION

The logistic function of a company must integrate this new security managerial dimension into its strategy and organization along the whole supply chain. The logistician should help managers to realize the importance of taking into consideration the security demands from the conception and development of the product to its final distribution to clients. Following the previous chapters in this paper on SCSM background, initiatives and measures, one should consider what kind of managerial implications SCSM is already having and is likely to have in the future. These issues are discussed below.

It is obvious that various industrial sectors have different backgrounds and attitudes towards SCSM. Some sectors have been traditionally governed by strict safety regulations in order to avoid explosions and other accidents (e.g. chemicals and petroleum), consumer problems (e.g. food and pharmaceuticals) etc. For them, many of the “new” SCSM measures are relatively easy, sometimes even trivial, to implement. Companies dealing with high value goods and / or easily tradable stolen goods (consumer electronics, tobacco etc.), and with dual-use type products also have a long tradition of highly protecting their assets. Therefore new SCSM initiatives might not require major investments

Most companies expect direct benefits from SCSM by immediate reductions in the following problem areas: theft, smuggling, counterfeit, and loss and damage, all of which are closely connected to the security measures described in the previous section. In addition, SCSM measures can help to avoid any kind of business disruptions, and to recover more quickly if something goes wrong, either due to internal or external factors; thus improving supply chain resilience. Such disruptions may include disruptions in supply, in transportation and at company facilities, freight breaches, and disruption in communications; they may be caused by accidents, fires, acts of nature, labour disputes, ordinary criminals etc. It is possible that reduction of such disruptions may happen already, thus justifying some of the SCSM investments. Besides reducing various risks in supply chains, SCSM may contribute to multiple collateral benefits, as presented in recent papers.

Governments, in particular Customs administrations seem to be eager to announce various types of benefits for supply chain actors who take proactive, highly compliant roles in their SCSM measures. In principle, the set of incentives could be grouped into the following three categories: (i) fast border flow under normal conditions, i.e. when no special threats are foreseen, "business as usual"; (ii) Fast border flow under special conditions, e.g. high alert and post-disaster situations; and (iii) Other possible incentives, e.g. tax incentives, connections with trade compliance / "traditional Customs incentives"; regulation consulting partnerships etc. However, for the time being it is still unclear how such potential benefits will evolve into measurable format.

6.0 CONCLUSION

One of the key questions regarding the future of SCSM is that of money: how much "it" will cost, and who will be the direct and indirect "payers". Interviews show that some MNC's seem to tolerate the introduction of some 10 to 30 USD security fees per container shipment quite well, by their LSP's, who claim such fees would cover in particular port and airport cost increases. At the same time, some companies notice that the "new" security fees are being added to their freight bills, even though the tasks were performed already before the past terrorist attacks. It is unlikely that a consensus will be reached as to how security should be priced – and by the end of the day, the final consumers will be the ones who pay.

Multiple concerns are being raised by various political, business and academic actors surrounding the broad picture and future of Supply chain security management (SCSM). Development agencies are highly concerned about the potential for introducing new trade barriers, affecting developing countries in particular, who may lack the resources and may not be able to afford the investments and operational costs set by SCSM requirements and expectations from industrial countries. Also SMEs at both developing and developed regions may find themselves in another "regulatory jungle" without resources to comply with all the SCSM aspects, and thus being cut out of part (or all) of international trade. In the worst case scenario, the trading world will be divided into two sections, "known parties" and "unknown parties", where the latter will find themselves finally being pushed out of business.

It is clear that the SCSM standardization work will continue to be driven by both governmental as well as business communities. It appears that an important part of this responsibility may be shifting to regional and global standardization bodies, such as CEN (European level) and ISO (global level). How to create and manage truly global, enforceable standards for the SCSM, remains an open question for future research and challenges various decision makers in the field. Also, the whole mechanism, from SCSM certification to auditing, remains open for the time being, including defining the main responsible government authority / authorities for the process, such as Customs, transport and other authorities.

It is evident that multiple expanded and new businesses are emerging around SCSM, while companies from various sectors, including aerospace and defence technologies, security technologies and services, Information Technology and services, shipment inspection and trade compliance services, management consulting etc., are seeking for new business and revenue opportunities. This includes new SCSM technologies, IT platforms, consulting, training and auditing services etc. It remains an open question as to which sectors and partnerships will manage to create the most reliable and cost efficient solutions and services for long-term success in the field. The pricing and financing of security, SCSM public-private-partnerships and other business and fiscal aspects remain a topic for future research.

Logistics should increasingly be the function capable of integrating the security dimension along the whole supply chain of a product or a service, in order to guarantee the reactivity and performance of any given company. Thus, the academic research community has a clear mission to bridge the gap between theoretical supply chain security studies, emerging security standards and practical managerial actions. One way of doing this is to proceed with pragmatic case studies on supply chain security implementation models in the context of real world supply chains.

REFERENCES

[1] Balen, John, et al. "Examining and resolving cybersecurity risks related to supply chain management ." International Journal of Science and Information System 13.17 (2022): 760-769.

[2] Boiko, Andrii, Vira Shendryk, and Olha Boiko. "Information systems for supply chain management: uncertainties, risks and cyber security." Procedia computer science 149 (2019): 65-70.

[3] Tang, Zuge, Behrad Zeinali, and Sarkew S. Abdulkareem. "Phase controlling of electromagnetically induced grating." Laser Physics Letters 19.5 (2022): 055204.

[4] Cheung, Kam-Fung, Michael GH Bell, and Jyotirmoyee Bhattacharjya. "Cybersecurity in logistics and supply chain management: An overview and future research directions." Transportation Research Part E: Logistics and Transportation Review 146 (2021): 102217.

[5] Zare, Saman, Behrad Zeinali Tajani, and Sheila Edalatpour. "Effect of nonlocal electrical conductivity on near-field radiative heat transfer between graphene sheets." Physical Review B 105.12 (2022): 125416.

[6] Ghadge, Abhijeet, et al. "Managing cyber risk in supply chains: A review and research agenda." Supply Chain Management: An International Journal 25.2 (2020): 223-240.

[7] Afroozeh, Abdolkarim, and Behrad Zeinali. "Improving the sensitivity of new passive optical fiber ring sensor based on meta-dielectric materials." Optical Fiber Technology 68 (2022): 102797.

[8] Melnyk, Steven A., et al. "New challenges in supply chain management: cybersecurity across the supply chain." International Journal of Production Research 60.1 (2022): 162-183.

[9] Zeinali, Behrad, and Jafar Ghazanfarian. "Turbulent flow over partially superhydrophobic underwater structures: The case of flow over sphere and step." Ocean Engineering 195 (2020): 106688.

[10] Lamba, Anil, et al. "Analyzing and fixing cyber security threats for supply chain management." International Journal For Technological Research In Engineering 4.5 (2017).

[11] Zeinali, Behrad, Jafar Ghazanfarian, and Bamdad Lessani. "Janus surface concept for three-dimensional turbulent flows." Computers & Fluids 170 (2018): 213-221.

[12] Boyes, Hugh. "Cybersecurity and cyber-resilient supply chains." Technology Innovation Management Review 5.4 (2015): 28.

[13] Golmohammadi, Amir-Mohammad, Negar Jahanbakhsh Javid, Lily Poursoltan, and Hamid Esmaeeli. "Modeling and analyzing one vendor-multiple retailers VMI SC using Stackelberg game theory." Industrial Engineering and Management Systems 15, no. 4 (2016): 385-395.

[14] Urciuoli, Luca, et al. "Supply chain cyber security–potential threats." Information & Security: An International Journal 29.1 (2013).

[15] Hadiana, Hengameh, Amir Mohammad Golmohammadib, Hasan Hosseini Nasabc, and Negar Jahanbakhsh Javidd. "Time Parameter Estimation Using Statistical Distribution of Weibull to Improve Reliability." (2017).

[16] Urciuoli, Luca, et al. "Supply chain cyber security–potential threats." Information & Security: An International Journal 29.1 (2013).

[17] Zavareh, Bozorgasl, Hossein Foroozan, Meysam Gheisarnejad, and Mohammad-Hassan Khooban. "New trends on digital twin-based blockchain technology in zero-emission ship applications." Naval Engineers Journal 133, no. 3 (2021): 115-135.

[18] Kumar, Subodha, and Rakesh R. Mallipeddi. "Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions." Production and Operations Management 31.12 (2022): 4488-4500.

[19] Bozorgasl, Zavareh, and Mohammad J. Dehghani. "2-D DOA estimation in wireless location system via sparse representation." In 2014 4th International Conference on Computer and Knowledge Engineering (ICCKE), pp. 86-89. IEEE, 2014.

[20] Sobb, Theresa, Benjamin Turnbull, and Nour Moustafa. "Supply chain 4.0: A survey of cyber security challenges, solutions and future directions." Electronics 9.11 (2020): 1864.

[21] Bahrami, Javad, Mohammad Ebrahimabadi, Sofiane Takarabt, Jean-luc Danger, Sylvain Guilley, and

Naghmeh Karimi. "On the Practicality of Relying on Simulations in Different Abstraction Levels for Pre-Silicon Side-Channel Analysis." 2022.

[22] Gupta, Nikhil, et al. "Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks." IEEE Access 8 (2020): 47322-47333.

[23] Sadi, Mehdi, Yi He, Yanjing Li, Mahabubul Alam, Satwik Kundu, Swaroop Ghosh, Javad Bahrami, and Naghmeh Karimi. "Special Session: On the Reliability of Conventional and Quantum Neural Network Hardware." In 2022 IEEE 40th VLSI Test Symposium (VTS), pp. 1-12. IEEE, 2022.

[24] Pandey, Shipra, et al. "Cyber security risks in globalized supply chains: conceptual framework." Journal of Global Operations and Strategic Sourcing (2020).

[25] Bahrami, Javad, Mohammad Ebrahimabadi, Jean-Luc Danger, Sylvain Guilley, and Naghmeh Karimi. "Leakage power analysis in different S-box masking protection schemes." In 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 1263-1268. IEEE, 2022.

[26] Luo, Suyuan, and Tsan-Ming Choi. "E-commerce supply chains with considerations of cyber-security: Should governments play a role?." Production and Operations Management 31.5 (2022): 2107-2126.

[27] Zalnejad, Kaveh, Seyyed Fazlollah Hossein, and Yousef Alipour. "The Impact of Livable City's Principles on Improving Satisfaction Level of Citizens; Case Study: District 4 of Region 4 of Tehran Municipality." Armanshahr Architecture & Urban Development 12.28 (2019): 171-183.

[28] Yeboah-Ofori, Abel, and Shareeful Islam. "Cyber security threat modeling for supply chain organizational environments." Future internet 11.3 (2019): 63.

[29] Zalnezhad, Kaveh, Mahnaz Esteghamati, and Seyed Fazlollah Hoseini. "Examining the Role of Renovation in Reducing Crime and Increasing the Safety of Urban Decline Areas, Case Study: Tehran's 5th District." Armanshahr Architecture & Urban Development 9.16 (2016): 181-192.

[30] Wolden, Mark, Raul Valverde, and Malleswara Talla. "The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system." IFAC-PapersOnLine 48.3 (2015): 1846-1852.

[31] Hadi, Narges, Jessica L. Spott, and Raegan Higgins. "Underrepresented Students' Experiences in STEM at Community Colleges: A Qualitative Exploration of Self-Identified Challenges and Supports." Journal of The First-Year Experience & Students in Transition 34.2 (2022): 65-82.

[32] Smith, Grafton Elliot, et al. "A critical balance: collaboration and security in the IT-enabled supply chain." International journal of production research 45.11 (2007): 2595-2613.

[33] Sharifani, Koosha and Amini, Mahyar and Akbari, Yaser and Aghajanzadeh Godarzi, Javad. "Operating Machine Learning across Natural Language Processing Techniques for Improvement of Fabricated News Model." International Journal of Science and Information System Research 12.9 (2022): 20-44.

[34] Boyson, Sandor. "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems." Technovation 34.7 (2014): 342-353.

[35] Amini, Mahyar, et al. "MAHAMGOSTAR.COM AS A CASE STUDY FOR ADOPTION OF LARAVEL FRAMEWORK AS THE BEST PROGRAMMING TOOLS FOR PHP BASED WEB DEVELOPMENT FOR SMALL AND MEDIUM ENTERPRISES." Journal of Innovation & Knowledge, ISSN (2021): 100-110.

[36] Amini, Mahyar, and Aryati Bakri. "Cloud computing adoption by SMEs in the Malaysia: A multi-perspective framework based on DOI theory and TOE framework." Journal of Information Technology & Information Systems Research (JITISR) 9.2 (2015): 121-135.

[37] Amini, Mahyar, and Nazli Sadat Safavi. "A Dynamic SLA Aware Heuristic Solution For IaaS Cloud Placement Problem Without Migration." International Journal of Computer Science and Information Technologies 6.11 (2014): 25-30.

[38] Amini, Mahyar. "The factors that influence on adoption of cloud computing for small and medium enterprises." (2014).

[39] Amini, Mahyar, et al. "Development of an instrument for assessing the impact of environmental context on adoption of cloud computing for small and medium enterprises." Australian Journal of Basic and Applied Sciences (AJBAS) 8.10 (2014): 129-135.

[40] Amini, Mahyar, et al. "The role of top manager behaviours on adoption of cloud computing for small and medium enterprises." Australian Journal of Basic and Applied Sciences (AJBAS) 8.1 (2014): 490-498.

[41] Amini, Mahyar, and Nazli Sadat Safavi. "A Dynamic SLA Aware Solution For IaaS Cloud Placement Problem Using Simulated Annealing." International Journal of Computer Science and Information Technologies 6.11 (2014): 52-57.

[42] Sadat Safavi, Nazli, Nor Hidayati Zakaria, and Mahyar Amini. "The risk analysis of system selection and business process re-engineering towards the success of enterprise resource planning project for small and medium enterprise." World Applied Sciences Journal (WASJ) 31.9 (2014): 1669-1676.

[43] Sadat Safavi, Nazli, Mahyar Amini, and Seyyed AmirAli Javadinia. "The determinant of adoption of enterprise resource planning for small and medium enterprises in Iran." International Journal of Advanced Research in IT and Engineering (IJARIE) 3.1 (2014): 1-8.

[44] Sadat Safavi, Nazli, et al. "An effective model for evaluating organizational risk and cost in ERP implementation by SME." IOSR Journal of Business and Management (IOSR-JBM) 10.6 (2013): 70-75.

[45] Safavi, Nazli Sadat, et al. "An effective model for evaluating organizational risk and cost in ERP

implementation by SME." IOSR Journal of Business and Management (IOSR-JBM) 10.6 (2013): 61-66.

[46] Amini, Mahyar, and Nazli Sadat Safavi. "Critical success factors for ERP implementation." International Journal of Information Technology & Information Systems 5.15 (2013): 1-23.

[47] Amini, Mahyar, et al. "Agricultural development in IRAN base on cloud computing theory." International Journal of Engineering Research & Technology (IJERT) 2.6 (2013): 796-801.

[48] Amini, Mahyar, et al. "Types of cloud computing (public and private) that transform the organization more effectively." International Journal of Engineering Research & Technology (IJERT) 2.5 (2013): 1263-1269.

[49] Amini, Mahyar, and Nazli Sadat Safavi. "Cloud Computing Transform the Way of IT Delivers Services to the Organizations." International Journal of Innovation & Management Science Research 1.61 (2013): 1-5.

[50] Abdollahzadegan, A., Che Hussin, A. R., Moshfegh Gohary, M., & Amini, M. (2013). The organizational critical success factors for adopting cloud computing in SMEs. Journal of Information Systems Research and Innovation (JISRI), 4(1), 67-74.

[51] Khoshraftar, Alireza, et al. "Improving The CRM System In Healthcare Organization." International Journal of Computer Engineering & Sciences (IJCES) 1.2 (2011): 28-35.