

Barriers and Opportunities In Cyber Risk And Compliance Management For Data-Driven Supply Chains

Williams Afrifah
Secure Cyber Systems
Research Group,
WMG, University of
Warwick
Williams.Afrifah@warwick.ac.uk

Gregory Epiphaniou
Secure Cyber Systems
Research Group,
WMG, University of
Warwick
Gregory.Epiphaniou@warwick.ac.uk

Nikolaos Ersotelos
School of
Mathematics and
Computer Science
University of
Wolverhampton
N.Ersotelos@wlv.ac.uk

Carsten Maple
Secure Cyber Systems
Research Group,
WMG, University of
Warwick
CM@warwick.ac.uk

Abstract

In today's highly competitive market, where globalisation, mass production, and specialisation characterise the interconnected industrialised society, integrated Supply Chains (SCs) are more important than ever. Decision-makers rely on precise SC data, and even the slightest interruption in the data flow can substantially impact the quality of the decisions. This dependency has inadvertently driven device connectivity towards an Industrial Internet of Things (IIoT) approach in the complete interconnection paradigm. While interconnectivity between devices has accelerated, IIoT and Industry 4.0, SC security measures have not kept pace. This conflict is exacerbated further where there is a need to process Personal Data produced by IIoT systems while maintaining data Confidentiality, Integrity and Availability (CIA). This paper provides an extensive review of academic sources and consulting reports and presents a comprehensive analysis of the relevance of personal data in managing Industry 4.0 SC complexity and visibility. The paper further examines the role that advancements in Blockchain and artificial intelligence (AI) can play in mitigating SC security management risks.

1. Introduction

Information is the primary engine of business decision-making on a strategic, tactical, and operational level [1]. Consequently, the volume of information and the data produced by, accessible to, and collected by businesses is rapidly increasing [2]. This is a problem for businesses since it makes it more difficult to identify and extract the most critical information needed for business and supply chain management. The term "Big Data" was coined to describe information assets characterised by such a high volume, velocity, and variety that they require

specific technology and analytical methods to be transformed into value [3]. Big Data is having a significant impact on many aspects of our society. Industrial organisations and scientific disciplines alike have seen the development of applications and technologies designed to handle Big Data and harness it for various purposes. While harnessing the power of Big Data via technology can be of great benefit to businesses, it is essential to ensure that any Personal Data flowing through Big Data processing systems is appropriately safeguarded. According to the Information Commissioner's Office (ICO), Personal Data is information relating to natural persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information. Applying appropriate security control measures to protect the Confidentiality, Integrity and Availability (CIA) of Personal Data can be challenging, especially where the fast development of technology and processing platforms outpaces the establishment of clear regulations, principles, and guidelines for various contexts of data processing [4]. These challenges of Personal Data management are especially pertinent in the context of data-driven Supply Chains (SC). Modern SC management systems can automatically bring together data from multiple sources and coordinate orders, updates, modifications, and tracking information in real-time. As such, they frequently handle Big Data rapidly in order to achieve business objectives in a timely manner. Personal Data is often incorporated into business processes that underpin these complex systems.

In that sense, a Supply Chain (SC) failure no longer refers to a material or product shortage or delayed availability. Businesses that do not manage their SC properly risk compromising the quality, innovation, and reputation of their products and suffering from

Personal Data breaches, information misuse, reputational damage, and legal charges for non-compliance [5]. As a result, SC failures may have a direct effect on corporate performance, shareholder returns, and financial sustainability. A recent study indicated that SC disruption can result in up to 30% decrease in shareholder returns. According to the authors, 84% of global supply chains faced at least one severe disruption over the previous year [6].

Moreover, the increased impact of SC failures, the probability of a failure occurring has increased dramatically over the past few decades. This is due to the fact that SCs have become extensively complex, spanning further across the globe and consisting of entities, each with its own objectives and strategies that may belong to several SCs. Therefore, if an entity exposes its SC system to unattended risks, its failure can affect the rest of SCs systems with which it interacts. Consequently, it is essential to correctly define and manage SC risks relating to the flow of Personal Data through multiple processing systems. Ultimately, such risks evolve and become more prevalent with time. They can derive by macro conditions that refer to disasters or instability out of the control of the SC entities or by intra-SC or intra-company disorders [7]. Examples include, but are not limited to, the increased complexity which globalisation has brought to SC systems, the lack of visibility among entities' communication, the dangers posed by uncooperative suppliers, the reluctance to commit to social performance improvement, lack of personal data protection, and inadequacies of risk assessment strategies [8]. Businesses must therefore comprehend risks to their Personal Data holdings, classify them, evaluate them, and develop appropriate mitigations. This requires a deeper understanding of operational models and/or business processes, as well as strengthening technical capabilities, implementing appropriate information security and data protection measures, and leveraging the technological advancements brought to supply chain management (SCM).

This paper offers a review of SC management barriers and risks in Industry 4.0, and looks at the role that emerging technologies, such as Blockchain and AI (artificial intelligence) can play in reducing SC security risks. The remainder of this paper is structured as follows: Section 2 delves into the emergence of Industry 4.0 and the ramifications for conventional supply chain management systems and procedures. Section 3 examines the major risks and challenges facing the SC industry now and in the future. In Section 4, we discuss the emerging technologies SC management, while Section 5 concludes this paper.

2. Evolution of I4.0 SC Management

The exponential growth of new generation computing and technological tools such as cloud edge computing, the Internet of Things (IoT), Big Data, cyber-physical systems (CPS), machine learning (ML), and artificial intelligence (AI) has transformed organisations by lowering operational costs, increasing product quality, and enabling faster and more reliable delivery [9]. There is little doubt that the rapid development of global competition has, both favourably and adversely, affected almost every marketplace that offers goods or services, regardless of the size of the companies involved [10]. According to Shahnawaz [10], global competition has produced an upward pressure on organisations to look for new markets and sourcing options to reduce their production cost, improve their products' quality and delivery services, and specialise in their core competency. This boost of global competition has driven many developments in Information and Communication Technology (ICT) innovations and even forced governments to take political measures regarding trade barriers, making it easier for companies to link with external entities and operate as a virtually integrated organisation.

SC management in Industry 4.0 exemplifies this latest level of development. The coordination of materials, information and logistics flows in corporate networks is primarily automated and reliant on digital technologies [11]. Transforming SC management into a digital process enables companies to track the entire SC in real-time. This makes it possible to spot risks, track orders, transits, or the warehouse status, thus minimising out-of-stock situations. To reach this degree of sustainability, all organisations that comprise the SC must be willing and able to exchange accurate data in a timely manner, ensuring a smooth, uninterrupted flow of information. If this requirement is not fulfilled, then the whole SC lifecycle could be at significant risk [12]. Since companies must process increasing volumes of data from their various suppliers, manufacturers, clients, and stakeholders as efficiently as possible, data management is critical in addressing the multiple challenges in SC systems. This is especially important in the case of Personal Data, where a careful balance must be struck between processing efficiency and appropriate protection. Industry 4.0 has brought about significant changes to these data-driven processes by using recent technological advances.

This systematic industrial digitalisation necessitates appropriate methodologies and data structures for

collecting, processing, and sharing relevant and accurate Personal Data securely and safely. Given that a circular economy should attempt to minimise the SC lifetime and boost resource efficiency, detecting and addressing information sharing barriers, as well as assessing and mitigating cyber risks and threats, become critical in optimising operations and related system losses. The use of artificial intelligence and machine learning capabilities in SC re-configuration may open the door to a slew of new threats and broaden the attack surface for astute adversaries. This may result in new and updated attacks that compromise personal data security and privacy, decreasing firms' ability to profit from data processing and knowledge generation.

3. Supply Chain risks and risk management

Due to the increasing likelihood and consequences of interruptions in SC resulting from security vulnerabilities being exploited, SC risk management is seen as a vital aspect in ensuring the profitability and continuity of SC partners. Given the range of events or situations that might influence SC entities, as well as the scope and complexity of SCs, defining, managing, and mitigating SC risks is becoming more challenging. Failure to do so effectively may have a negative effect on all organisations involved, including a drop in share prices due to poor product quality, delivery delays, equipment damage, and ultimately reputational damage [13]. In the following sections, we explore how Personal Data flowing through a SC can be impacted by the primary types of SC security risks. We also provide recommendations for technical and strategic solutions to help businesses become more resilient.

3.1. Supply chain complexity and visibility

SCs are networks consisting of globally interconnected entities and subsystems, which interact with each other by exchanging information. This information may contain Personal Data, as well as sensitive system data that must be protected appropriately. Effective collaboration between these entities and the secure management of Personal Data across the end-to-end systems is critical to SC's success [14]. Accurate information sharing between SC components in a timely manner is crucial for streamlining SCM execution, resulting in increased performance, responsiveness, and flexibility while reducing uncertainty among SC partners [15]. SCM must be customer-oriented since current knowledge of market trends and consumer preferences is essential to

a business's success [16]. As businesses are compelled to rethink their marketing strategies and to really listen to and interact with their customers, the visibility and openness of consumer Personal Data becomes a critical factor in marketing decision-making, ultimately deciding the company's market performance.

Managing, negotiating, evaluating, and optimising these relationships adds complexity to SC. Complexity also grows with the application of industry standards, which often require new integrations and compatibility assurance or due to strategic alliances, mergers, and acquisitions [17].

The first strategic capability of a company is to discriminate between necessary and unnecessary complexity. While necessary complexity adds value to the company, unnecessary complexity increases the risk and costs without benefit. A company needs to define, prevent, and avoid unnecessary complexity and manage the necessary complexity.

In a holistic supply chain, SC risk management does not reside solely within an individual company's boundaries. The fundamental principle of SC risk management is the pragmatic development of a holistic strategic relationship with suppliers, who are deemed to be trusted partners, with a mutual aim of achieving excellence for both parties benefit. Recent research [18] stressed the critical importance of evaluating risk management along the lines of three major themes, (i) mutual objectives, (ii) problem resolution, and (iii) dedication to continuous improvement.

Transparency is crucial for SC enterprises to recognise, monitor, and respond to potential risks and establish a more effective risk and sustainability management programme. By gaining visibility into a SC partner's end-to-end operations, including Personal Data management, periodic independent cyber security reviews, technical risk assessment, threat profiling, and documented procedures and operational work instructions, a business can detect and mitigate threats and vulnerabilities [19]. Transparency also benefits riskless mature suppliers since open and collaborative relationships strengthen their operations, competitiveness, and viability in the face of adversity. One of the most significant issues is that most organisations lack insight into their supply chain processes, leaving them open to worldwide exposures. Mondragon [20] reports that 50% of major manufacturers lack visibility beyond their closest partners, while just 9% report total visibility, encompassing insight into all suppliers and partners. According to the researchers, visibility becomes even more crucial for organisations aiming to globalise their products, as inventories and information asset management become more complicated. Figure 1

illustrates how the complexity of a SC influences and organisation's visibility and management. Visibility necessitates a deeper knowledge of the type of data, their sensitivity and criticality to the company in terms of the effect of a compromise. This assessment is key to ensuring a better understanding of the Personal Data involved for the secure ingestion, processing, transmission, storage, and destruction of the data throughout the SC paradigm. An audit is one of the most effective ways to get a better insight of how Personal Data is safeguarded across SC organisations. A Supplier Self-Assessment, often known as an informal preliminary audit, is a method for SC organisations to establish openness and confidence. Once the supplier completes a self-assessment, the results can immediately indicate weaknesses, gaps, or non-conformance with other SC entities [21]. Even though auditing is a highly valuable technique for gaining awareness in the SC, it may also be utilised for illegal business rivalry in specific circumstances. Suppliers could use their size, dominance and/or impact to compel a smaller supplier into compliance for auditing. In contrast, in similar situations, larger enterprises will decline to be audited by their customer and deliberately withhold the right to audit them by way of a service level signed contract [22].

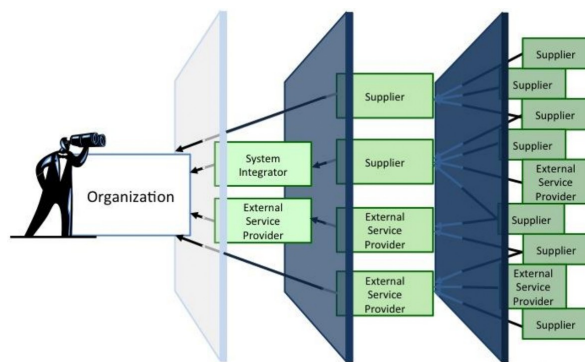


Figure 1. Relationships with System Integrators, Suppliers, and External Service Providers NIST 800-161 ICT SCRM Risk Management

Audits require resources and increase operational costs for the collaborating parties, especially where offshore auditing is required.

One challenge associated with auditing is that some suppliers, fearing commercial penalties, do not always act in the best interests of a transparent audit process. In many cases, they try to hide their poor practices and inadequate or even non-existent controls in contracts, which may result in customers seeking reparation by way of penalty clauses.

According to Saeed [23], SC visibility is defined as the awareness of and control over specific information related to the product orders and physical shipments,

including transport and logistics activities, and the statuses of events and milestones that occur prior to and in-transit. SC visibility can be a major setback and a bottleneck regarding information security, assurance, governance and adherence to standards, policies, and regulations. In part due to the fact that many SCs are globally dispersed networks of dependents, increasing visibility might be both expensive and time-consuming. To this end, data-driven SC management, assisted by IIoT, applied analytics, AI, and ML and Blockchain can enhance the end-to-end transparency across the SC [24]. These technology-led leveraging platforms, integrated with the SC management systems and logistics control, act as 'a nerve centre' for the flow of supply chain data and improve real-time visibility of inter-SC operations. As digital supply chain integration improves delivery tracking, innovative measures are more likely to enhance information security and management visibility.

3.2. Social performance management in SC

In a broader sense, social performance can be understood as the measurement of social issues that trigger concerns in society. Measuring SC performance with social indicators is not an easy task. Social issues have a very dynamic nature, and social indicators are difficult to enforce across the entire supply chain. A definition for social problems in the SC is provided by Morais [25] as the "product/process-related aspects of operations that affect human safety, welfare and community development". In line with this definition, some metrics for social issues include health and safety incidents, health and safety practices, product safety, economic welfare, and growth.

The ability of organisations to identify and manage social performance issues is vital to the continued sustainability of the SC. Developing effective methods to evaluate, compare, benchmark, and connect behaviours to sustainability indicators is essential for any sustainability program's success [26]. The SC view is vital because sustainability risks begin with suppliers, not goods. It is possible for organisations to overlook unethical labour practices and unsustainable processing packaging and transportation operations. Inbound and outbound logistics are also being evaluated for their environmental effect, with businesses trying to reduce variables including distance, transit, cargo volume and batch size. Transparent and efficient monitoring/measurement are essential to communicate performance both internally and externally successfully and to have a trajectory towards progress [26]. Both in the UK and internationally, it has been noticeable that firms are unwilling to allocate money to the social performance

management process where there is already a contract in place, and delivery expectations are high. However, there are drawbacks to this policy; without appropriate measures, the SC process would be riddled with irregularities making it harder to implement the necessary tasks. Nishinaga [27] states that companies do not acknowledge their contribution to adverse impacts on workers. For larger enterprises, globalisation has seen more outsourcing of business functions. However, different countries have unique laws, regulations, and demographics, which may or may not affect SC.

3.3. Inadequate risk assessment processes

The vast economic and political growth has undoubtedly contributed to an increase in SC complexities as they extend across more international borders. The impact of disruptions that remained locally isolated in the past, such as natural disasters, political turmoil, piracy, and regional economic crises, nowadays spread and affect interconnected SC entities directly and indirectly. To provide an example, Eisenman [28] alludes to the COVID-19 epidemic in China, which caused the manufacture and distribution of new iPhone models to be delayed as a result of the closure of factories, assembly locations, and distribution outlets in the Apple organisation's SC. Had more careful consideration been given to the risks involved in operating in China, the disruption may have been managed more effectively. Pettit [29] cites another case; following Japan's 2011 earthquake and tsunami that led to a nuclear calamity. The automotive giant Toyota had its production reduced by 40,000 vehicles, costing an estimated \$72 million in daily profits. In an age of intense diversity and uncertainty when markets are highly unpredictable, firms operating in supply chains that may be geopolitically compromised constantly exist on the edge in order to meet customer expectations; consequently, they must adopt effective risk management mitigation strategies [30].

The necessity of risk assessment processes to proactively identify, manage and increase resilience against risk is widely recognised by enterprises and the supply chains. However, improving the resiliency against SC risks requires radical strategic decisions to prioritise it as a business requirement and change the operating model and organisational structure to support it. SC management requires a clear governance structure to support the respective operations, skilled resources with clearly defined accountabilities and ownership, and clearly defined processes and SC management systems and analytics support.

An essential pillar in bridging the gap in SC Risk

Assessments processes is the establishment of SC Security and Assurance Programmes. Organisations must establish robust Supply Chain Security Assurance Programmes to ensure that all suppliers are subject to rigorous periodic security risk assessments before and throughout the entire lifecycle of the chain [31]. Any residual risks from the Supplier Assurance Programme must be effectively managed and periodically reviewed to ensure the risk is kept within the organisation's risk appetite.

Adopting Supply Chain Risk assessment processes, business structures and culture must be communicated and acknowledged with the SC partners. In addition to that, Zsidisin [32] refers to the importance of adopting an Early Supply Involvement (ESI) as a way to reduce the probability of a SC disruption risk and mitigate the subsequent impacts. ESI is a practice of collaboration between SC partners where the manufacturer involves the supplier at an early stage of the product development process. Even though SC risk assessment procedures do not guarantee the absence of SC failures, they minimise the impact and accelerate the recovery, in case of exposure, by planning and implementing comprehensive business continuity plans. Worth noting that the essence of conducting a risk assessment is to protect an organisation's information assets, including Personal Data. Security Assurance Programme is vital to protect information assets that are valuable to the business, and Personal Data is one such information asset.

3.4. Information security and data protection challenges

With the advancement of data-driven processes, SCs is faced with security threats at any given time. These attacks may be carried out by internal threat actors (employees) or external threat actors such as Foreign Intelligence Services, Organized Crime, Hackers, etc. For example, insiders may collude with external criminals by providing information identifying weak points or revealing authentication passwords - criminal actions which can generate significant issues for companies or even put them at risk of bankruptcy. Furthermore, Urciuoli [33] explains that implementing advanced information technology systems in SC means that various parties, e.g., shippers and logistics, can share and analyse large amounts of data to make daily activities and operations more flexible and efficient. Such information may be related to purchase orders, bills of materials, shipping instructions, warehouse packing lists etc. Unfortunately, this process, which allows many entities to access information, comes with many security challenges. While most businesses devote considerable money to resolving

interoperability challenges when linking disparate legacy systems, they neglect security risks. Typically, the source of cyber-attacks is overlooked until a specific organisation is impacted.

Different data types (e.g., personal customer records) reside in many places in a data-driven SC, and their protection depends on a combination of encryption, integrity protection, and data loss prevention techniques. As organisations move towards cloud computing and mobile access, care must be taken to limit and report data theft while also mitigating the effects of data compromise. Some companies fail to identify and isolate their most valuable information assets from less business-critical and publicly available information on their internal networks, or they fail to regulate the appropriate access rights in line with security best practices.

Internal users in many environments have access to all or most critical assets like those that manage and control physical systems, such as Supervisory Control and Data Acquisition (SCADA). Once attackers penetrate a network, they can easily find and remove important information such as sensitive system details and personal data, cause physical damage, or disrupt operations with little resistance. Jansen [34] stressed the need for organisations to understand its sensitive information, where it resides, and who needs access to it; similarly, Casino [35] advocates putting together lists of the key types of data and their overall importance.

In order to create a comprehensive data classification scheme, organisations should consider the value of their data assets and the restrictions that must be applied to their access and use. Once the criticality and sensitivity level of the information has been identified, it can be further subdivided based on its impact if it were compromised. Upon determining the sensitivity levels, a data inventory or map should be created according to the data's applications [36]. Different security controls can then be implemented to protect assets according to their classification. The network then needs to be segmented so that systems of the same sensitivity level are separated from systems with higher sensitivity levels; firewalls can also control access to each segment. Access to data should be based on job requirements and on a need-to-know basis or by applying the principle of least privilege. Job requirements should be created for each user group to determine what information the group needs access to perform their jobs. Detailed logging should be turned on for servers to track access and allow for security personnel to examine incidents in which data was improperly accessed.

3.5. Legal and regulatory challenges

The rapid growth of global competition and connectivity has resulted in many organisations relying on various Commercial Off-the-Shelf (COTS) products from countries with different legal and regulatory measures and data protection restrictions [37]. Unfortunately, very little has been done regarding legal and regulatory measures to avoid uncertainty and curb potential exploitation by suppliers. The requirement for alignment with key stakeholders, businesses or institutions on legal and regulatory measures helps in the negotiation of agreements and builds confidence within SC and partners [38]. A recent analysis [39] remarked that standardisation could play a positive role as a single source of informal rules to regulate the public realm and bring benefits in terms of knowledge, credibility, and risk reduction through accountability and predictability.

In today's data-driven settings, SC management rules are being developed to improve both business and individual controls by increasing transparency and permission requirements [39]. Additionally, the regulations include restrictions governing the profiling and individual rights when conducting business on a global scale. As a result, they clarify and expand the duties of regulators and processors via additional accountability requirements [40].

Coercive pressure of a regulatory environment, especially regarding IT estate, would influence SC processes.

For example, Gruschka [41] states that privacy issues cause alarm in data driven SCs due to the requirement to store, process and often share large volumes of information. One of the challenges is finding the right way to protect personal data by limiting the amount of information shared with third parties involved in the chain. Since any security weaknesses can make an organisation vulnerable to data privacy compromises, companies are responsible for ensuring that contracts contain clauses that safeguard personal data. Moreover, regular vendor risk assessments should be conducted to ensure that all possible threats and vulnerabilities immediately identified and addressed accordingly. To that target, in January 2012, the European Commission suggested reforms of the EU's 1995 data protection rules to strengthen online privacy rights [42]. Recent examples of reform have been Fair Information Practices, designed to harmonise with recently introduced privacy laws, and the European Union Data Protection Directive (DPD).

It is apparent that companies face challenges in using SC management data to avoid legal issue related to personal data and privacy violations. Using standard

privacy preservation techniques, such as cryptography and obfuscation, the vast amount of data processed and exchanged may be inefficient. Therefore, it is necessary to effectively distinguish between personal and non-personal data in line with the Information Commissioner's Office (ICO) guidelines.

Preserving data privacy is becoming increasingly complicated considering significant data processing activities needed for SC management integration, record linking and sharing of often unstructured IIoT data. Given that this data may contain personally identifiable information (PII) or private information, such integration processes could result in serious privacy violations. In addition to that, even if sensitive personal data are obscured to meet users' privacy requirements, SC data management operations could lead to the generation of new identification patterns concatenating original sensitive data that must remain protected.

3.6. Strategic planning of SCRM and SCM based on ICT

The COVID-19 pandemic has exposed most organisations' SC risk management weaknesses. More than 94% of one thousand companies surveyed by Zhu et al. [43] saw disruptions on their SC, and 75% reported negative or economic solid impacts on their businesses. The main reason is due to the multiple and long-term national lockdowns and the significant restrictions on travel which have minimised the flow of raw materials and finished goods. The impact was substantial, especially to those firms which were dependent on China trade. In their attempt to support their local industries, most governments have provided treatment to the employees who have been infected and financial support for industrial firm's sustainability [44]. While the magnitude of the effects cannot be foreseen since this was not a normal risk occurrence, reality has shown that the majority of the difficulties are not new.

Today, more and more organisations realise the need to focus carefully on the strategic planning of their SCRM as it helps them resolve localised and exceptional global risks, reduce vulnerability, and ensure long-term survival. These evaluations must prioritise health to maintain the workforce healthy and productive via the introduction of new alternative modes of work, such as protective gear, and the establishment of alternative operational measures, such as remote work and Q&A helplines.

Secondly, during a pandemic event, the organisation must be adaptable to create alternative goods depending on current market needs and raw material availability. Transport risks must be assessed as part of

procurement, management, and governance processes.

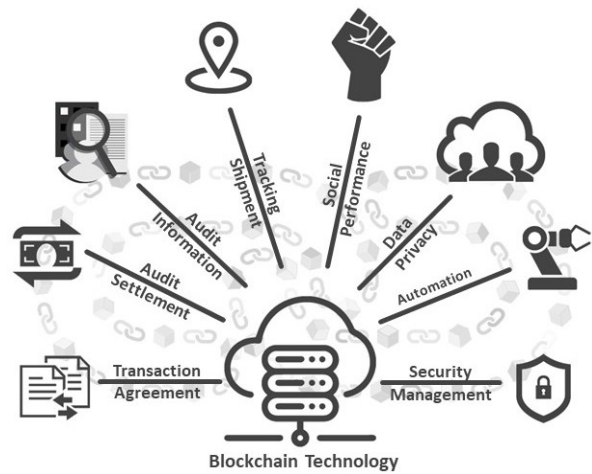


Figure 2. Blockchain In Industry 4.0, Supply Chain Management: Use Cases

4. Emerging technologies in data-driven SC management

With the use of IIoT and Blockchain, technological tools must develop a fully trusted SC network through information sharing for the accurate development of standardised risk assessments and quantification tools. Over the past decade, it has been shown that Blockchain technologies have tremendous potential to revolutionise supply chain management and address security, data protection, and privacy concerns regardless of geographical location[45]. Blockchain is a decentralised and distributive technology that can provide confidentiality, integrity, and data availability of the transactions. Thus, it can improve the transparency and visibility of SC management data flow, enable process automation, eliminate intermediaries, and enable real-time tracking through traceability, privacy, and data management techniques [46]. Blockchain forms a sequence of blocks that hold a complete list of transaction records, much like a general public ledger. Although several limitations have been recorded, such as the restrictions on a block's size and its transaction rate, those are not significant issues for validating records. The innovative idea behind Blockchain is that all transactions are stored in a decentralised distributed ledger within the communication environment.

According to Epiphaniou [46], this distributed ledger is produced collaboratively using strong cryptographic protection, is validly distributed amongst all peers, and can offer an immutable audit trail and transaction

history for all the different data levels accessed modified within the SC environment. That business logic is often executed with transactions using distributed applications.

Recently, several approaches have been launched and published in the public domain that utilise Blockchain technologies to regulate and control the flows of Personal Data; hence privacy and anonymity were preserved [47]. Most importantly, because of its decentralised structure, Blockchain appears to be resilient against data outages and to provide a certain degree of data contingency within the communication network. Data reliability often depends on the controls imposed for creating the transactions by specified authorities. Therefore, it is imperative to identify the exact means by which Personally Data is created before it is placed onto a Blockchain network. Peterson [48] stated that some aspects surrounding the authenticity of data are often considered outside the scope of a Blockchain operation. Therefore, defensive measures must always be taken outside the Blockchain network (Commercial Product Assurance CPA by CESG, a UK Government scheme designed to assure commercial security products).

The use of blockchain technology in the provision of SC in Industry 4.0 has gained popularity owing to its capacity to create and deploy distributed ledgers comprised of various data structures essential to SC management [49]. The technology promises to achieve global visibility to individualised SC activities, making it entirely changeless and distributable within the supplier's network by leveraging strong cryptographic primitives to establish trust among peers and industry partners. Access to such Personal Data can only be achieved efficiently, securely, and verifiably without modification to an existing block that encapsulates a particular supplier's record, which cannot be tampered without modifying all subsequent blocks. Figure 2 demonstrates the Blockchain's relevant use cases in data-driven SC management.

Therefore, unauthorised modifications are easily detectable with Blockchain and, to a certain extent, attributable. Indicatively, the Blockchain network offers strong integrity and immutability; however, it also has a perpetual data storage capacity which might conflict with the UK General Data Protection Regulation (GDPR). Other notable challenges include the size of the data required to be stored together with existing searching capabilities offered by Blockchain, particularly when hashes will be regarded as Personal Data by the Information Commissioner's Office (ICO). In principle, the deployment of Blockchain technology must reflect on specific privacy issues linked to extant ICT systems to ensure that the "need to know" and "least privilege" principles are strictly adhered to in the

SC management [50]. Also, the viewing and retrieval permissions are often complicated to establish on the premise that different SC members frequently share data processing and viewership. This is also true for Cloud service provisions, which have seen unprecedented deployment and processing of Personal Data and organisation's data in recent times due to convenience, savings, and near-real-time access.

Certain limitations and security implications have been recorded and challenged regarding the integrity of handling Personal Data, such as conventional cryptographic algorithms used and the application of legacy access control systems. Economies of scales are slowly emerging to cyber-criminals who seek to benefit financially from the theft of Personal Data.

Big-Data based IIoT systems, which get widely adopted within the SC management systems, collect large amounts of data from sensors and processes them in centralised servers. Centralised AI algorithms are utilised for various tasks, such as demand optimisation and production planning based on data from IIoT sensors, which, together with other Edge devices, are the main data collection points. However, the drawback to centralised AI algorithm training, based on IIoT data, is that information privacy may be compromised. During training, attackers could gain access to the generated data because IIoT sensors are so sensitive that they can make physical processes visible when conducted in industrial sites. Moreover, this information can be used to launch physical cyber-attacks against industrial control systems (ICS).

To reduce the risk of privacy loss, the distributive nature of the Federated Learning approach offers the capability of more secure AI training models. If FL is utilised to gain access to Personal Data, potential attackers would have to penetrate multiple systems at the edge rather than at a single centralised core, making the attack attempt much more difficult.

Federated Learning works in different network topologies: the first being a centralised topology in which the clients using IoT or edge devices - synchronise with a server, download a master model, and then perform iterations of the stochastic gradient descent algorithm using samples from their local data copies. Following this, the resulting weight update vector is communicated to the server, thereby updating the master model. The original centralised topology, which had an inconsistent data distribution problem, has been improved by Sattler [50], who proposed a clustered topology. The second topological type is wholly distributed and works in a peer-to-peer fashion. Savazzi [51] propose fully distributed (or serverless) FL algorithms by iterating model updates consensually. This approach has the advantage of better

scalability compared to the centralised and clustered topologies and avoids a single point of failure. However, in an industrial setting, a fully decentralised topology may not be desirable because organisations need to control the data flow and access.

5. Conclusion

SC has been undergoing tremendous changes over the last few decades, moving away from purely operational logistics activities and towards automated end-to-end data-driven processes. Data have become the most critical resource for many modern companies as information technology advances. This paper has provided a comprehensive overview of the relevance of Personal Data in managing Industry 4.0 SC complexity and visibility. We have emphasised the role that advancements in emerging technologies such as Blockchain, Federated Learning and artificial intelligence (AI) can play in mitigating inefficiencies in SC data management via enhanced transparency, decentralisation, optimisation, and sustainability. Further work in SC management security domain is required to assist firms to build and execute these secure technologies to eliminate vulnerabilities.

References

- [1] Rai, Arun, Ravi Patnayakuni, and Nainika Seth. "Firm performance impacts of digitally enabled supply chain integration capabilities." *MIS quarterly* (2006): 225-246.
- [2] McAfee, Andrew, et al. "Big data: the management revolution." *Harvard business review* 90.10 (2012): 60-68.
- [3] De Mauro, Andrea, Marco Greco, and Michele Grimaldi. "A formal definition of Big Data based on its essential features." *Library Review* (2016).
- [4] Boyd, Danah, and Kate Crawford. "Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon." *Information communication & society* 15.5 (2012): 662-679.
- [5] S. Abdul Ganiyu, D. Yu, C. Xu, and P. Mongo, "The impact of supply chain risks and supply chain risk management strategies on enterprise performance in Ghana," *Open Journal of Business and Management*, vol. 08, pp. 1491–1507, 01 2020.
- [6] "Supply chain resilience report 2021," BCI 2021.
- [7] Davies, P., Parry, G., Alves, K. and Ng, I. (2020) How additive manufacturing allows products to absorb variety in use: empirical evidence from the defensive industry. *Production Planning and Control*. ISSN 0953-7287.
- [8] Vidrová, Zdenka. (2020). Supply chain management in the aspect of globalisation. *SHS Web of Conferences*.74.04031.
- [9] Ivanov, Dmitry & Dolgui, Alexandre & Sokolov, Boris. (2018). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *International Journal of Production Research*.57.1-18. 0.1080/00207543.2018.1488086.
- [10] S. Shahnawaz and A. Kulakli, "Big data in mitigating systemic supply chain risks: A systems perspective with case studies," *Journal of Business Research - Turk*, vol. 10, pp. 15–32, 08 2018
- [11] M. J. Ferrantino and E. E. Koten, "Understanding supply chain 4.0 and its potential impact on global value chains," *Global Value Chain Development Report2019*, p. 103, 2019.
- [12] S. Luthra and S. Mangla, "Evaluating challenges to industry 4.0 initiatives for supply chain sustainability in emerging economies," *Process Safety and Environmental Protection*, vol. 117, 05 2018.
- [13] D. Kuupiel, B. Tlou, V. Bawontuo, P. Drain, and T. Mashamba-Thompson, "Poor supply chain management and stock-outs of point-of-care diagnostic tests in upper east region's primary healthcare clinics, Ghana," *PLOS ONE*, vol. 14, p. e0211498, 02 2019.
- [14] R. Narasimhan and S. Talluri, "Perspectives on risk management in supply chains," *Journal of Operations Management*, vol. 27, pp. 114–118, 04 2009.
- [15] Force, Joint Task. "Risk management framework for information systems and organisations." *NIST Special Publication 800* (2018): 37
- [16] G. Saunders, Andrew. (1994). Supplier Audits as part of a Supplier Partnership. *The TQM Magazine*. 6. 41-42. 10.1108/09544789410054028.
- [17] Davis, Edward Wilson, and Robert E. Spekman. *The Extended Enterprise: Gaining Competitive advantage through collaborative supply chains*. FT press, 2004.
- [18] Cao, Mei, and Qingyu Zhang. "Supply chain collaboration: Impact on collaborative advantage and firm performance." *Journal of operations management* 29.3 (2011): 163-180.
- [19] Sithole, Beverley, Sergio Guedes Sila, and Mirjana Kavej. "Supply chain optimisation: enhancing end-to-end visibility." *Procedia engineering* 159 (2016): 12-18.
- [20] A. Mondragon, C. Lalwani, and C. Mondragon, "Measures for auditing performance and integration in closed-loop supply chains," *Supply Chain Management: An International Journal*, vol. 16, pp. 43-56, 01 2011.
- [21] Johnstone, Karla M., Chan Li, and Shuqing Luo. "Client-auditor supply chain relationships, audit quality, and audit pricing." *Auditing: A Journal of Practice & Theory* 33.4 (2014); 119-166.
- [22] Touboulic, Anne, Daniel Chicksand, and Helen Walker. "Managing imbalanced supply chain relationships for sustainability: A power perspective." *Decision Sciences* 45.4 (2-14): 577-619.
- [23] K. Saeed, M. Malhotra, and S. Abdinnour, "How supply chain architecture and product architecture impact firm performance: An empirical examination," *Journal of Purchasing and Supply*

- Management, vol. 25, 03 2018.
- [24] Garay-Rondero, Claudia & Flores, José Luis & Smith, Neale & Caballero, Omar & Aldrette-Malacara, Alejandra. (2020). Digital Supply Chain Model in Industry 4.0. *Journal of Manufacturing Technology Management*. 10.1108/JMTM-08-2018-0280/full/pdf?
- [25] D. Morais and J. Barbieri, "Social performance measurement for sustainable supply chain management," 05 2016.
- [26] Taticchi, Paolo, Flavio Tonelli, and Roberto Pasqualino. "Performance measurement of sustainable supply chains: A literature review and a research agenda." *International Journal of Productivity and Performance Management* (2013).
- [27] J. Nishinaga and F. Natour, "Technology solutions for advancing human rights in global supply chains," *Human Rights and Business Initiative*, vol. 1, no. 1, 2019.
- [28] Eisenman, David J. "Rereading Arrowsmith in the COVID-19 Oandemic." *Jama* 324.4 (2020): 319-320.
- [29] T. Pettit, K. Croxton, and J. Fiksel, "Ensuring supply chain resilience: Development and implementation of an assessment tool," *Journal of Business Logistics*, vol. 34, 03 2013.
- [30] D. A. Ghadge, W. Hendrik, and S. Seuring, "Managing climate change risks in global supply chains: A review and research agenda," *International Journal of Production Research*, vol. 58, 06 2019.
- [31] O. Tang and N. Musa, "Identifying risk issues and research advancements in supply chain risk management," *International Journal of Production Economics*, vol. 133, pp. 25–34, 09 2011.
- [32] G. Zsidisin and M. Smith, "Managing supply risk with early supplier involvement: A case study and research propositions," *Journal of Supply Chain Management*, vol. 41, pp. 44 – 57, 11 2005.
- [33] L. Urciuoli and J. Hintsä, "Adapting supply chain management strategies to security – an analysis of existing gaps and recommendations for improvement," *International Journal of Logistics Research and Applications*, vol. 20, pp. 1–20, 09 2016.
- [34] W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing," *Public Cloud Computing: Security and Privacy Guidelines*, vol. 800, 01 2012.
- [35] F. Casino, T. Dasaklis, and C. Patsakis, "A systematic literature review of Blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, 11 2018.
- [36] Dubey, Rameshwar, et al. "Explaining the impact of reconfigurable manufacturing systems on environmental performance: The role of top management and organisational culture." *Journal of cleaner production* 141 (2017): 56-66.
- [37] M. Zhao, "Supply reduction policy against new psychoactive substances in china: Policy framework and implementation," *International Journal of Law, Crime and Justice*, vol. 60, 12 2019.
- [38] B. Yuan and Y. Zhang, "Flexible environmental policy, technological innovation and sustainable development of china's industry: The moderating effect of environment regulatory enforcement," *Journal of Cleaner Production*, vol. 243, p. 118543, 09 2019.
- [39] C. Sene, *Fostering the Participation of Companies in Standardisation: A Soft Law Instrument to Reduce Risks – The Concept of Student Standardization Societies*, pp. 252–278. 01 2020.
- [40] I. Rubinstein, "Big data: The end of privacy or a new beginning?" *International Data Privacy Law*, vol. 3, pp. 74–87, 05 2013.
- [41] Gruschka, Nils, et al. "Privacy issues and data protection in big data: a case study analysis under GDPR." *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2018.
- [42] Christou, George. "European Union privacy and data protection policy." *The Routledge Handbook of European Public Policy*. Routledge, 2017. 179-190.
- [43] Zhu, M. Chou, and C. Tsai, "Lessons learned from the covid-19 pandemic exposing the shortcomings of current supply chain operations: A long-term prescriptive offering," *Sustainability*, vol. 12, 07 2020.
- [44] J. M. De Vet, D. Nigohosyan, J. Núñez Ferrer, A.K. Gross, S. Kuehl and M. Flickenschild, "Impacts of the covid-19 pandemic on eu industries Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, vol. 12, 2021.
- [45] Al-Zaben, Nasr, et al. "General data protection regulation complied blockchain architecture for PII management." *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*. IEEE, 2018.
- [46] Rogerson, Michael, and Glenn C. Parry. "Blockchain: case studies in food supply chain visibility." *Supply Chain Management: An International Journal* (2020).
- [47] G. Epiphaniou, P. Pillai, M. Bottarelli, H. Al-Khateeb, M. Hammoudeh, and C. Maple, "Electronic regulation of data sharing and processing using smart ledger technologies for supply-chain security," *IEEE Transactions on Engineering Management*, vol. PP, pp. 1–15, 01 2020.
- [48] K. Peterson, R. Deeduvanu P. Kanjamala and K. Boles, "A Blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, vol. 1, pp. 1–10, 2016.
- [49] Assunta Di Vaio, Luisa Varriale, *Blockchain technology in supply chain management for sustainable performance: Volume 52, 2020, 102014, ISSN0268-4012*.
- [50] F. Sattler, K.-R. Müller, and W. Samek "Clustered federated learning: Model-agnostic distributed multitask optimisation under privacy constraints," *IEEE Transactions on Neural Networks and Learning Systems*, vol. PP, pp. 1–13, 08 2020.
- [51] S. Savazzi, M. Nicoli, and V. Rampa, "Federated learning with cooperating devices: A consensus approach for massive iot networks," *IEEE Internet of Things Journal*, vol. 7, pp. 4641–4654, 01 2020.