DOI:

Journal of Computers and Intelligent Systems

Vol. 2, No. 1, 2024, pages 01 - 14

Journal Homepage:

https://journals.iub.edu.pk/index.php/JCIS/

Application Layer Issues and Challenges in Supply Chain 4.0

Zaima Mubarak[1*] Muhammad Zulkifl Hasan[2], Muzzamil Mustafa[3], Muhammad Zunnurain Hussain[4], Adeel Ahmad Siddiqui[5], Muhammad Atif Yaqub[6]

[1,5,6] Department of Computer Science National College of Business Administration and Economics, Lahore, Pakistan

[2]Faculty of Information Technology, Department of Computer Science, University of Central Punjab Lahore Pakistan

[3] Department of Artificial Intelligence, University of Management and Technology Lahore, Pakistan

[4]Department of Computer Science, Bahria University Lahore Campus, Pakistan

ARTICLE INFO

Article History:

Received:	May	01, 2024
Revised:	May	22, 2024
Accepted:	May	23, 2023
Available Online:	May	24, 2023

Keywords:

Supply chain management,
Supply Chain 4.0,
Industry Revolution IR 4.0,
Internet of things (IoT),
Wireless Sensor Networks (WSN's),
Application Layer

Classification Codes:

Funding:

This research received no specific grant from any funding agency in the public or not-for-profit sector.

ABSTRACT

This paper considers the cyber security hurdles which plague the supply chains in modern times, specifying the challenges in Supply Chain 4.0. The article discusses the unparalleled growth in the number of supply chain cyberattacks mentioned by famous specialists, for example, by Juhan Lepassaar and security specialists from IBM Security X-Force. It also underlines the crucial necessity of the effective defensive measures and efficient cooperation among involved stakeholders. Through highlighting the multifaceted essence of supply chain attacks, the paper emphasizes the paramount importance of vulnerability management and proactive security measures which are referred to as preventive measures are crucial in mitigating such attacks. Besides that, it touches upon the details of layer applications protocols and incoming network assaults, pointing out the core issues and campaigning for programs of research and development. Cybersecurity is a fundamental aspect of organizations of today. However, they face unique challenges, given the increasing complexity of modern supply chains. The paper's comprehensive analysis and practical recommendations constitute a strategic blueprint for organizations to build-up their cyber defense networks and effectively manage the intricacies of supply chain security. It has been revealed as a helpful instrument for comprehension and solving the causing risks in Supply Chain 4.0, while assuring the reliability and continuity of the industry, which operates in a data-driven and integrated manner.

OPEN ACCESS

© 2023 The authors published by JCIS. This is an Open Access Article under the Creative Common Attribution Non-Commercial 4.0

Corresponding Author's Email:

Citation:

1. Introduction

A supply chain is the ecosystem of resources required to create, manufacture, and distribute a product. In cybersecurity, a supply chain includes cloud or local storage, software and hardware, and distribution methods. Supply chain attacks doubled in 2021 compared to the last year. Lawmakers and the cybersecurity sector must move promptly due to a new trend. Therefore, defensive measures must be introduced as soon as feasible to avoid and react to dynamic supply chain risks while minimizing their impact. Through the cascading impact of supply chain assaults, threat actors may cause significant harm to enterprises and their consumers all at once," stated Juhan Lepassaar, Executive Director of the EU Agency for Cybersecurity. Member state achieved a comparable level of coordinated efforts at European Union, enhancing the EU's common level of cybersecurity"[1].

IBM Security is one of the most comprehensive security products in the industry. The portfolio backed by IBM Security X-Force allows businesses to manage risk. It has one of the largest security research and delivery sectors in the world with 150 billion+ events each day in over 130 countries and 10,000 security patents. In 2021, according to IBM Security's annual X-Force Threat Intelligence Index, malware and vulnerability predations combined to "imprison" organizations. It's wreaking havoc on global supply systems, making the industry the most vulnerable. Although phishing has been the most prevalent source of attacks last year, Identity Management X-Force saw a 33% spike in unpatched software attacks in 2021, which were the most popular point of entry for malware actors, accounting for 44% of ransomware attacks According to a study from 2022, ransomware offenders sought to "destroy" the basis of global supply chains in 2021 [2]. Figure 1 shows the threat landscape for supply chain attacks[3].

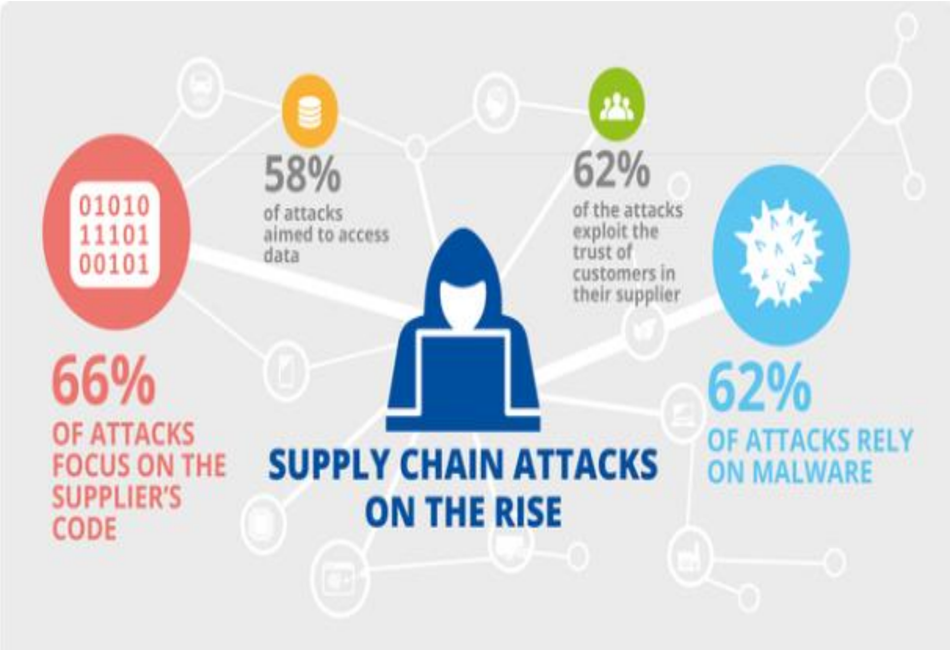
01010
11101
00101
58%
of attacks aimed to access data
62%
of the attacks exploit the trust of customers in their supplier
66%
OF ATTACKS FOCUS ON THE SUPPLIER'S CODE
SUPPLY CHAIN ATTACKS ON THE RISE
62%
OF ATTACKS RELY ON MALWARE

Figure 1: ***Threat Landscape for Supply Chain Attacks*****[3]**

Financial products and insurance have been dethroned after a long reign. According to a study from 2022, ransomware offenders sought to "destroy" the basis of global supply chains in 2021. Financial products and insurance were dethroned after a long reign. Attackers banked on the tremendous impact that disrupting industrial companies would have on their downstream supply networks, forcing them to pay the ransom[4]. Manufacturing businesses have been the subject of more ransomware than every industry, and attackers bet on the downstream supply chains being disrupted, forcing companies to pay the ransom. Vulnerabilities that now the market participants had not yet repaired or were unable to patch were responsible for 47% of industrial attacks, highlighting the importance of addressing vulnerability management[5]. Figure 2 explains the supply chain statistics in detail the figure shows the supply chain distribution stats, the common KPI's used for supply chain monitoring and the top tech priorities of supply chain professionals[6].

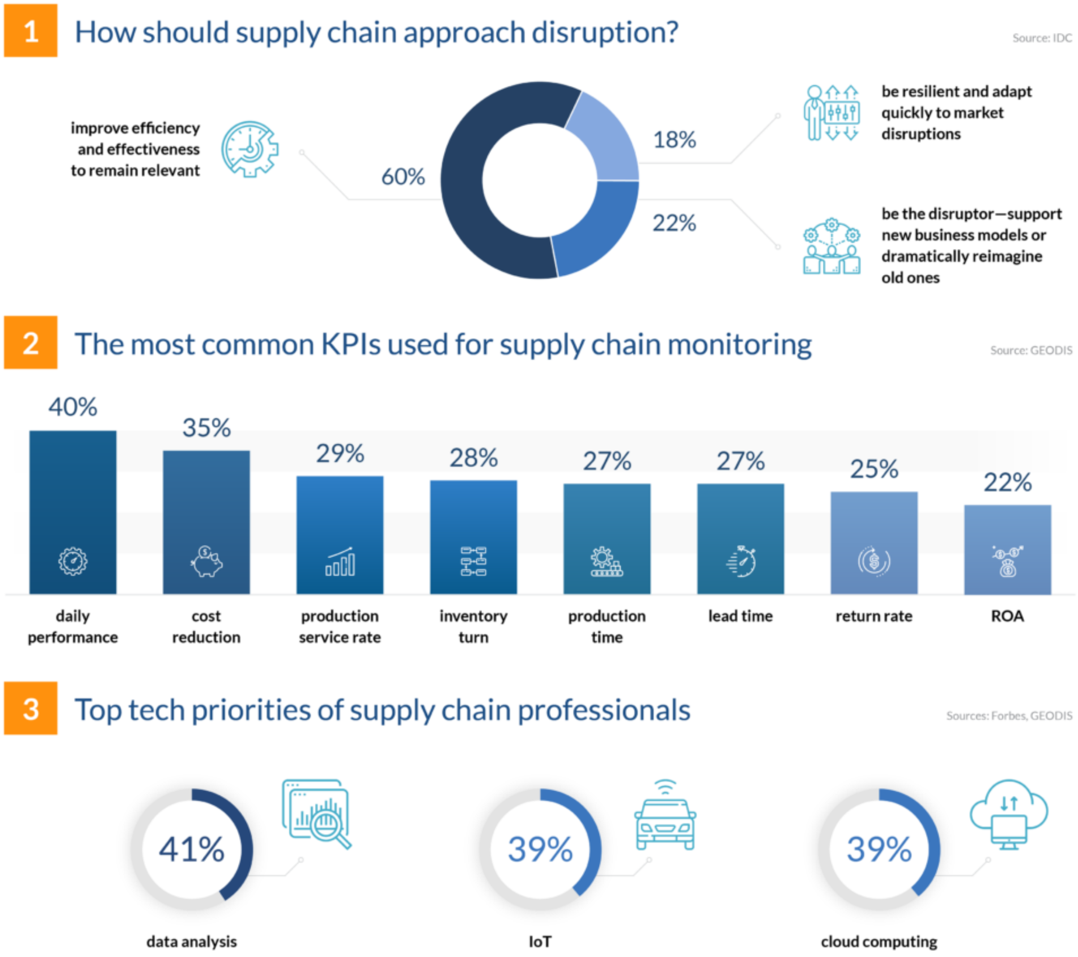

Figure 2: **Supply Chain Statistics**

The IBM Security X-Force is a group of security experts at IBM. Some of the most notable comments put forward are:

- **Ransomware Gangs Defy Takedowns**

Despite an increase in ransomware takedowns, ransomware remained the most common threat tactic in 2021, with ransomware teams exhibiting no signs of slowing down. According to the survey, a ransomware group's average lifespan before closing or renaming is 17 months.

- **Vulnerabilities reveal the biggest "Vice" of a company.**

According to X-Force, unpatched vulnerabilities triggered almost 50% of assaults in 2021 in Europe, Asia, the Middle East, and Africa, highlighting enterprises' main struggle– fixing vulnerabilities.

- **Early Warning Indicators of a Cloud Cyber Crisis**

With a 146 percent spike in Linux System ransomware code and a change to Docker-focused targeting, cybercriminals are building the groundwork to attack cloud infrastructures, possibly making it easier for additional threat actors to utilize. Advance Warning Signs of a Cloud Cyber Crisis With a 146 percent spike in new Linux ransom code and a move to Docker-focused targeting, cybercriminals are building the foundation to target cloud systems, possibly making it simpler for additional threat actors to utilize cloud environments for harmful reasons.

"Most cybercriminals want money. "They're seeking leverage now with ransomware," stated Charles Henderson, Head of IBM X-Force. "Businesses should know that weaknesses tie them up in knots, as ransomware perpetrators take advantage of this." This is a task that isn't binary. Because the attack is only expanding, organizations should operate under the premise that every risk in the environment has been addressed, rather than assuming that every vulnerability has been patched".[7]

○ Ransomware Organizations' "Nine Lives."

Ransomware gangs may start activating their disaster recovery in response to law enforcement's benefits achieved by ransomware takedowns. According to X-research, Force's a ransomware group's average lifespan until shutting down or renaming is 17 months. Ravil, for example, which was involved in 37% of any ransomware assaults in 2021, survived for four years after rebranding, implying that this will return after being taken down by an inter effort in mid-2021.

Making it more difficult to access vital data in cloud storage settings may help organizations manage, govern, and safeguard their workloads, as well as decrease threat actors' power in the case of a compromise. For some, weaknesses become an existential crisis.

○ Vulnerabilities Become an Existential Crisis

According to the X-Force research, the number of vulnerabilities reported in 2021 set a new high, with flaws in Industrial Control Systems increasing by 50% yearly. Even though there are around 146,000 vulnerabilities

Enterprises' vulnerability management difficulties will likely intensify as engineering and electronics expand and organizations get overloaded with inspection and upkeep needs, highlighting the significance of being able to function under the assumption of compromise and adopting a zero-trust approach to secure their architecture.

○ Attackers Target Common Grounds Among Clouds

Threat actors are also warned about in the paper for 2022. The threat actors' continuous investment in unique, previously unseen Linux malware is also a concern in the 2022 study, with statistics from Intezer suggesting a 146 percent growth in Linux ransomware with novel code. Businesses must focus on increasing insight into their hybrid infrastructures as attackers continue to seek ways to scale operations through cloud environments. Organizations can use hybrid cloud environments built on openness and interoperable for automated security response[8].

Figure 3 below shows the major issues and challenges withing the supply chain 4.0, most of the issues can be categorized into 4 main types of the cyber issues, data issues, information issues and information technology issues. These issues are further broken down into respective domains with are interconnected somehow.

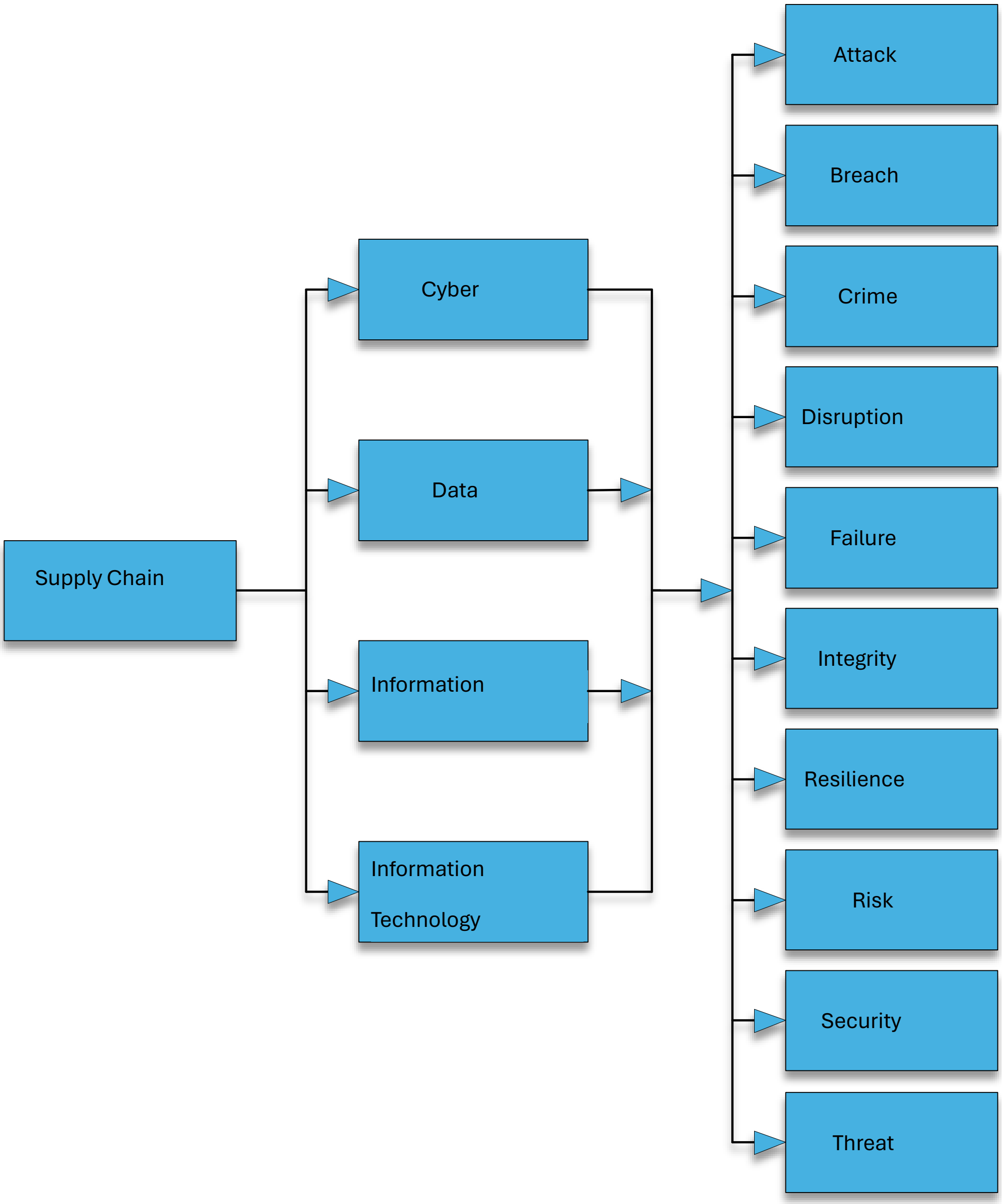

Figure 3: **Issues and Challenges in Supply Chain 4.0 management**

I. Why is a high level of cybersecurity insufficient?

Supply chain attacks may take months to execute, which involve attacking one or more suppliers before moving on to the client's final target. In many circumstances, an attack like this could go unreported for a long time. Attacks against supply chains, such as Advanced Persistence Threats (APT), usually cyber-attacks are concentrated, sophisticated, and costly, with attackers presumably planning of time. All these variables represent the degree of difficulty. All these factors present the enemies' level of intelligence moreover their determination to prosper. Even if the organization's defenses are strong, it might be exposed to a supply chain assault. The attackers find new arenas to enter companies by focusing only on suppliers. Moreover, as the impact of supply chain assaults on large consumers is endless, these attacks are becoming popular[9].

To hurt the targeted consumers in approximately 66% of the reported incidents, attackers focused on the code of the providers. This highlights the need for their efforts to check third-party code and technology before implementation to ensure that it has not been interfered with or modified. Customer data was targeted particularly in around 58 percent of the supply chain incidents according to Personally Identifiable Information (PII) statistics and intellectual property. Suppliers were unaware or failed to recognize how they were hacked in 66% of supply chain hacks investigated. However, only 9% of consumers who were attacked due to supply chain hacks knew about the incident. This emphasizes the maturity difference between suppliers and end-users regarding cybersecurity event reporting[10].

The infrastructure as a service (IaaS) resource of the cloud can be managed by platforms. Open-source cloud systems have grown in popularity because of their rapid development. Because they are open and accessible, some of them can be used in place of commercial clouds. Some previous publications merely compare the essential characteristics of open-source platforms, leaving out some recently announced functionality. Open Nebula maintains virtual infrastructure to create Service Clouds that are public, private, public, and hybrid[11]. Virtualization, storage, networking, monitoring, and security are all managed by it. With key ideals including openness, cooperation, and innovation, Open Nebula lets you construct and operate virtualized enterprise data centers and IaaS clouds (Wen, 2014). AWS EC2 and EbS APIs are provided by Open Nebula, as well as a self-service portal for cloud users. It comes with a powerful CLI. It comes with a strong CLI that looks like UNIX commands. User, group, and role administration, as well as access control lists, auditing, and isolation at various levels, provide security[12].

Developers devised ways to manage their resources using native OpenStack RESTful APIs. For the time being, OpenStack also provides "AWS EC2 compatibility API and supports AWS S3 API". Security is a critical aim of cloud computing; many experts are racing to learn more about it. OpenStack and OpenNebula respect security as a top priority, taking numerous steps to assure it. Keystone is a new project that provides services for authenticating, managing, and approving users and accounts in OpenStack. It connects with existing authentication systems and enables universal authentication across all projects. It includes terms like "user, authentication, token, tenancy, and role," among others[13]. We can see from the above that OpenStack spent a lot of time developing an excellent technique to ensure security and reliability. As we can see from the above, OpenStack has spent a lot of work developing a sound security system that focuses on authentication and authorization. It separates users into relatively small groups and assigns distinct duties to them. A user logs in and may be given tokens to access resources. The user inherits these rights and privileges from the role to which it belong. Nova-Network, of course, uses VPN (Virtual Private Network) connectivity and firewall regulations. OpenNebula is also working on several security features for its cloud. OpenNebula, like OpenStack, has a safe and efficient "Users and Groups Subsystem" for pluggable authorization and authentication via passwords and other methods. Examples are RSA keycode pairs, X509 certificates[14].

II. What are major Application Layer Protocols and Network Attacks in Supply Chain IR 4.0?

Figure 4 shows the major application layer protocols that are being used in supply chain 4.0. the figure also states the respective the network security attacks that hit and affects the protocol performance and reliability. Table 1 is the advance version of the diagram the table elaborates the popular application layer protocols and the network attacks that specifically targets these layers. The description and cause of the attacks are also stated along with the certain preemptive measures supply chain managers and network security professionals can take to avoid and stop the network attacks.

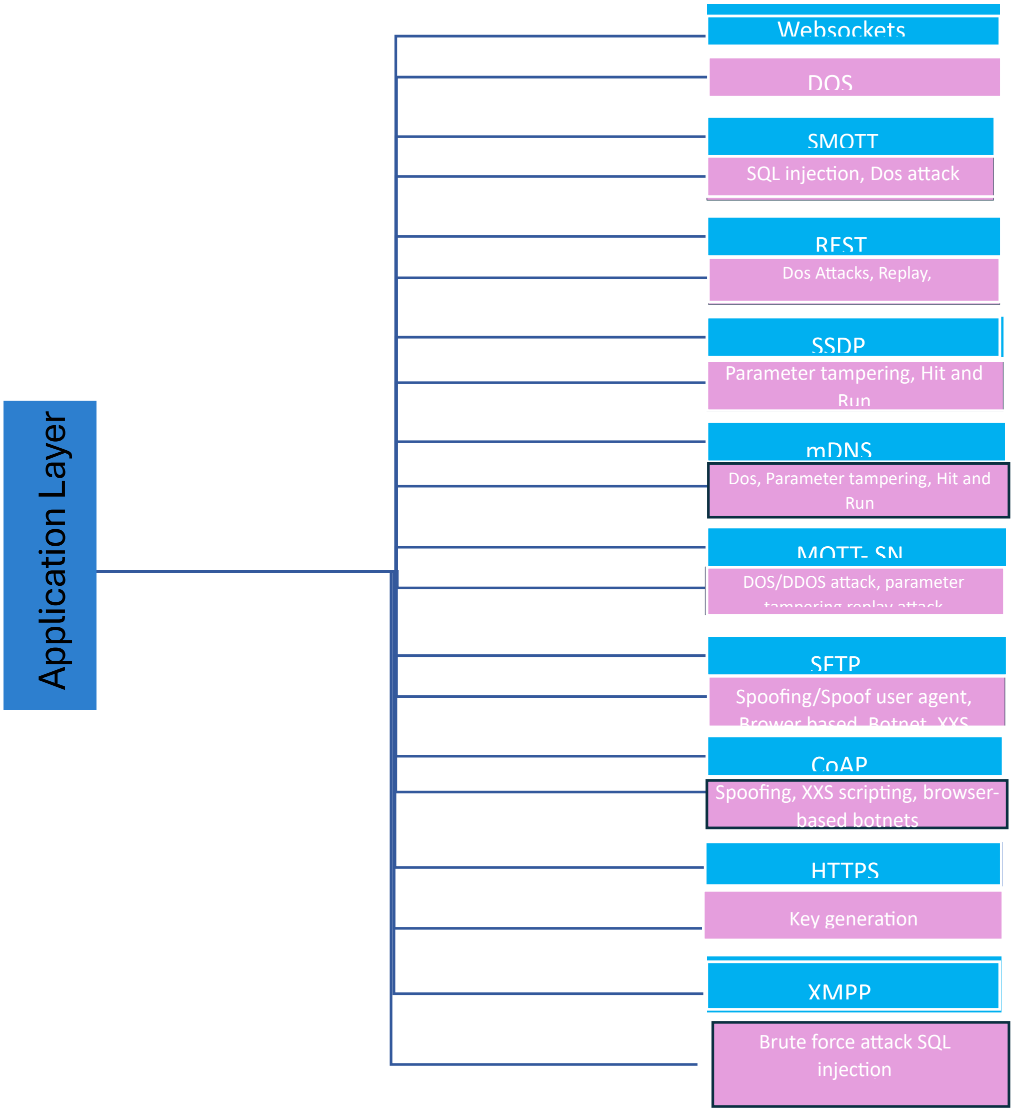
Application Layer
Websockets
DOS
SMQTT
SQL injection, Dos attack
REST
Dos Attacks, Replay,
SSDP
Parameter tampering, Hit and Run
mDNS
Dos, Parameter tampering, Hit and Run
MQTT- SN
DOS/DDOS attack, parameter tampering replay attack
SFTP
Spoofing/Spoof user agent, Brower based, Botnet, XXS
CoAP
Spoofing, XXS scripting, browser-based botnets
HTTPS
Key generation
XMPP
Brute force attack SQL injection

*Figure 4: **Application Layer protocols and attacks in supply chain 4.0***

2. Related Works:

Table 1: Network Attack and security precautions for Application Layer Protocols in IR 4.0 Supply Chain

Application Layer Protocol	Description	Attacks	Description	Security Precaution
WebSockets[15]	WebSockets stipulate a bidirectional, full-duplex communications network which operate over HTTP and are in fact an application layer protocol that enable a client and server to keep a constant connection through Single TCP/IP socket link.	DOS attack	A denial-of-service (DoS) assault in which the attacker tries to prevent the intended users of a computer system from accessing it by interfering with the system's normal operation. The fundamental objective is to exceed the capacity of the computer being attacked,	Access control and create a denial-of-service response plan Consider DDoS-as-a-Service, safeguard the network infrastructure, and use cloud computing.

			which causes denial-of-service for any further requests.	
SMQTT (Smart Message Queuing Telemetry Transport)[16]	A single message is encrypted and distributed to several nodes using attribute-based encryption. The master secret key is given during configuration to subscribers and publishers that register with the brokerage. Before being made public, data is encrypted, and the very same master key is also used to decode it later.	Cross site scripting, SQL injection, Dos attack	Attacks known as **cross-site scripting (XSS)** include injecting malicious scripts into often reputable and innocent websites. When a hacker uses an online application to send harmful code to a specific end user, frequently in the form of a browser side script, the assault is known as an XSS attack. A network is subjected to an **injection attack** when malicious code is introduced, retrieving all the content from either the servers and sending it to the attacker. An attacker can alter a database query issued by an application by using SQL injection. In some circumstances, an attacker may edit or remove this data, causing the content or activities to be permanently changed.	Detection forms for self-inflicted attacks and vulnerabilities for SQL injection Putting An SQLi Detection Tool to Test and Using It Check the accuracy of the users' inputs Enforced Formulated Arguments And Parameterization Make advantage of stored procedures in the database. Boost Operating System And Application Security Limit your movement to lessen the attack's surface. Long URLs are prohibited.
SSDP (Simple device recovery protocol)[17]	It is an Internet protocol-based network protocol for advertising and identifying network resources and presence data. It accomplishes so without the need of any static network host configuration or server-based configuration protocols like Dynamic Host Configuration Protocol (DHCP) or Domain Name System (DNS).	Parameter tampering, Hit and Run attacks	**Parameter tempering** is a sort of Man-in-the-Middle attack that involves changing application data, including authentication tokens and privileges, by fiddling with parameters that are communicated between the client and server. A hostile user who intends to utilize the application for personal benefit. A H**it-and-Run attack** uses intermittent bursts of massive frequency cyberattacks or injects malicious packets, yet the effects are long-lasting and spaced at random. By bringing down the host server, it intended to prevent a user from using a service.	Coding techniques, browser safety Check the accuracy of the users' submissions, Enforced Formulated Expressions And Parameterization with complex URLs and Activated firewalls.

mDNS (multicast Domain Name Server)[18]	A name resolution system called multicast DNS (mDNS) was created targeting subnetworks without a local name server. A multicast is a type of communication where a particular signal is broadcast simultaneously to several recipients. It is a zero-configuration solution that utilizes the operational semantics, packet formats, and unicast Domain Name System programming interfaces (DNS).	Dos, Parameter tampering, Hit and Run attacks, botnets, Spoofing	A **botnet** is a collection of computers with internet access that have been infected with malware and are under the control of hackers, enabling them to engage in criminal activity. Cybercriminals utilize specialized Trojan infections to obtain access, then deploy centralized command software to carry out serious harmful actions. **Spoofing** is the practice of portraying correspondence from an anonymous source as coming from a confirmed, reliable source. A computer can spoof an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server, which is a simple kind of spoofing, or it can be more sophisticated.	It is crucial to update the operating system, authenticate the browser, validate user inputs, enforce parameterized queries and parameterization, and block extended URLs. using behavioral analysis to determine how unusual each request is from the norm to spot changes in site-specific traffic. Use spoofing detection tools, authenticate users and apps, and implement traffic filtering with deep packet inspection. Protocols that are encrypted and authenticated ought to be used.
REST (Representational State Transport) [19]	The HTTP protocol is used by the web-based REST protocol. A Web service that adheres to these guidelines is referred to as RESTful. Such a Web service must implement a stateless protocol and a predetermined set of actions to give its Web services in a textual form and make them accessible for reading and updating.	Dos Attacks, Replay attacks, SQL injection	A **replay attack** occurs when a hacker listens in on a secure network connection, deflects it, and then purposefully delays or retransmits it to trick the recipient into acting in accordance with the hacker's wishes. Replay attacks provide an additional risk since, after intercepting a communication out from network, an attacker would not necessarily need technical knowledge to decode it.	The company's information technology assets now include an intrusion protection system, Creating a plan for emergency management Regular penetration tests must be performed. Following a security compromise, stopping the replay assault Establishing an Incident Response Team
XMPP (Extensible Messaging and Presence protocol)[20]	An open standard for instant messaging, presence, multi-party chat, video and audio calls, connectivity, lightweight middleware, content syndication, and generalized XML data transportation is the Extensible Messaging and Presence Protocol (XMPP). The communications protocol XMPP is reliable, scalable, decentralized, flexible, and functional.	Brute force attack SQL injection,	A **Brute force** is a dictionary attack is a type of attack that tests hundreds or millions of plausible candidates, or a broad range of phrases, to create potential passwords to determine the passphrase or decryption key for a cypher or authenticating system.	Use robust encryption techniques, secure passwords, access control, intrusion monitoring, and firewall implementation. Both input validation and exit sanitization or data compression filter data as it enters and leaves the system, respectively. Use required response headers, a content

				security policy, server-side sanitization, and client-side sanitization.
MQTT-SN (Message Queuing Telemetry protocol for Sensor Networks)[21]	The MQTT-SN IoT communications protocol is an enhanced version of a MQTT (Message Query Telemetry Transport) standard designed for effective operation in large low-power IoT sensor networks. It will reduce the expense per unit and, as a response, the overall rate of service by lowering the amount of data sent. To fix this, transmit data only when necessary.	Dos/DDos attack, parameter tampering, replay attack,	An intentional attempt to stop daily traffic to a targeted server, service, or network by saturating the target or its neighboring networks with Internet traffic is known as a distributed denial-of-service (DDoS) assault. A DDoS assault is comparable to an unexpected traffic congestion that clogs the road and prevents regular traffic from getting to its destination.	Establish firewalls, allocate responsibilities, and establish a denial-of-service response plan. Use the Cloud to safeguard your network's infrastructure and consider DDoS-as-a-Service.
CoAP (Constrained application protocol)[22]	The Constrained Application Protocol (CoAP), a particular web transport protocol for usage among constrained nodes and constrained networks, is used in the Internet of Things. Even over confined networks with poor bandwidth and availability, CoAP is a protocol that enables simple, constrained devices to communicate with the Internet of Things. Common applications for machine-to-machine (M2M) technology include smart energy and building security.	Spoofing, cross cite scripting, browser-based botnets,	In cryptography, a related-key attack is a type of cryptanalysis during which the attacker may watch how a cypher behaves under multiple distinct keys, the values of which are initially unknown, however the attacker is aware of some mathematical connection connecting the keys.	Use robust encryption techniques, secure passwords, access control, intrusion monitoring, and firewall implementation. Both input validation and exit autoclaving or data compression filter data as it enters and leaves the system, respectively. Use required response headers, a content security policy, server-side sanitization, and client-side sanitization.

What are Supply Chain 4.0 limitations and Require research development?

Table 2 below gives an extensive description of most of the Issue currently being observed in the supply chain 4.0 industry along with the limitations within the recent work and progress being carried out. Moreover, the correct research development required by the current industry to reduce their issues for a more enhanced and effective performance paradigm.

TABLE 2: Supply Chain 4.0 Issues, Limitations and Development suggestion

Issue	Limitation	Required Research development
Robustness and fault tolerance [23]	Defective sensor Sensor failure Attack Network failure	Any assault or change in the environment might target malfunctioning sensors and cause power loss failures, making sensor networks susceptible. Even if a few nodes fail in such critical situations, the network must continue to function. Throughout WSN operations, sensor nodes continually lose energy. Therefore, fault-tolerant designs are necessary for WSN to operate effectively.
Security [24]	Network attacks Eavesdropping Access control Privacy	Researchers must devise a method to protect the system from unauthorized access, and the hub must continue to exercise access control. Prior to transmission to the transfer hub or base station, detected information should be encrypted for privacy and accuracy. It must adjust to the different security norms.

Limited Resources [25]	Power Memory Internet Security	For efficient, safe, and quick data transfer that also extends the life of WSN, it is necessary to design low-power, low memory, regulated security, and dependable transmission medium.
Operating System [26]	Complex systems Management Administration of resources	The sensor's OS should be a straightforward programming environment with a focus on memory management that is less complicated. It should also be application specific, equipment free, and suitable for use in an urgent environment. Application validation activities including designing, licensing, and administration quality should be the main emphasis of the application engineers.
Quality of Service (QoS) [27]	Network management resource management	Organizational involvement, interactive sensors, effectiveness, an assessment of sensor precision, latency, and delay precision are some of the Precise constraints for the QoS application. Additionally, WSN's QoS can withstand node cancellation and extension. As the location of the organization tends to change and information management is ambiguous, it is difficult to track QoS boundaries for sensor networks.
Deployment [28]	Node organization Data security Deployment strategy	Sensor hubs are extremely dense, and several simultaneous transmission attempts may cause a network to get blocked. Uninformed yield or an absence of data observation will arise from the case's insufficient or sparse configuration of sensor hubs. If hubs are dispersed randomly, the self-setup attribute is required.
Tampering [29]	Physical tampering Network tampering	Security is ensured through trustworthy network management, monitoring, and security procedures that stop or restrict physical and network threats. The WSN is impenetrable, and the network's functionality is unaffected.

Dataset:

For detailed analytics we took the “Application Layer DOS Attack” dataset from Kaggle, the dataset consists of over 1000 instances and 78 no of attributes. The first step is to load the dataset and get data analytics for the columns using the MatplotLib python library. Figure 5 shows the plot per column distribution of the dataset where per column distribution of instances for selected columns is plotted. Figure 6 shows the data correlation plot for the entire dataset that states the correlation of every column to another, the correlation helps to find out the dependencies of columns with one another the correlation value lies between -1 to 0 to 1. Figure 7 states the scatter plot of the dataset that indicates the value distribution of the instances in accordance with the attributes moreover the plot also states the density of the instances with the attributes as well.

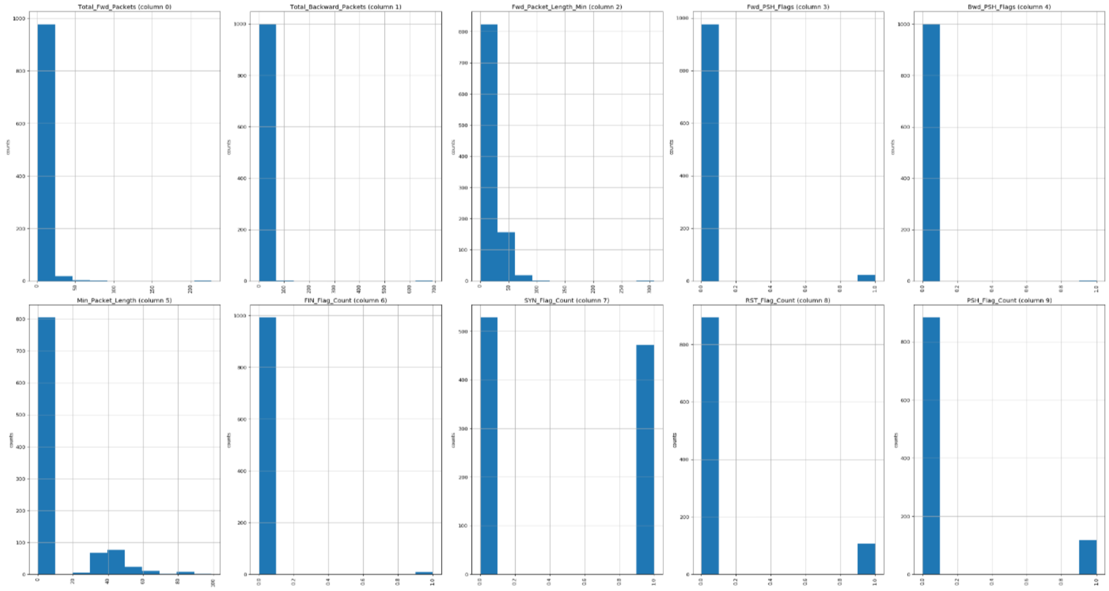

*Figure 5: **Column Distribution of Application Layer Dos Attack dataset***

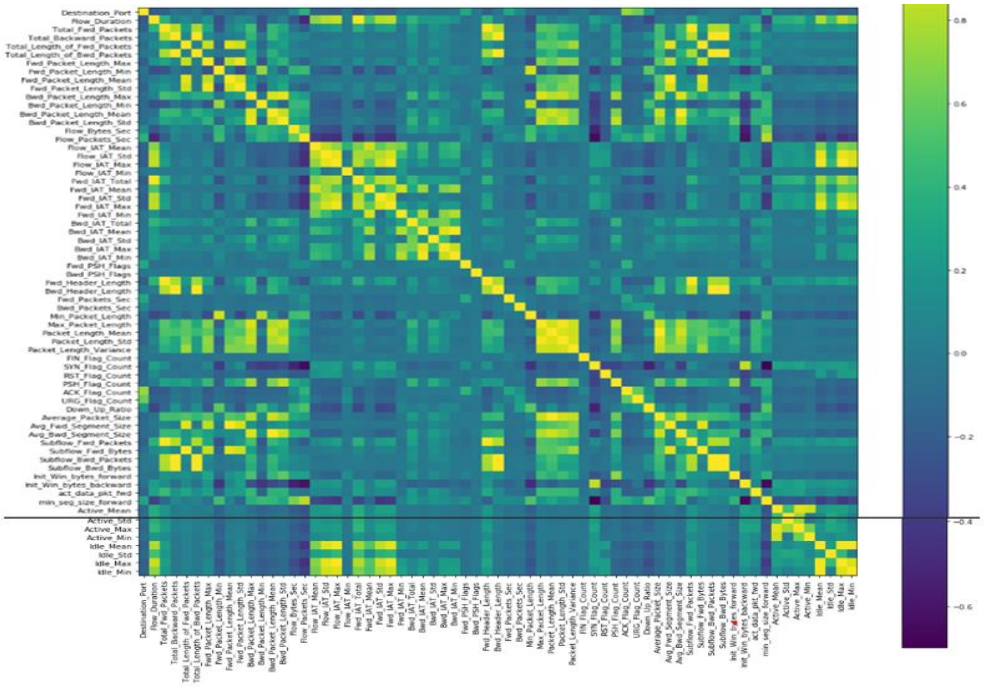

Figure 6: **Data Correlation Matrix For Application Layer DOS Attack Dataset**

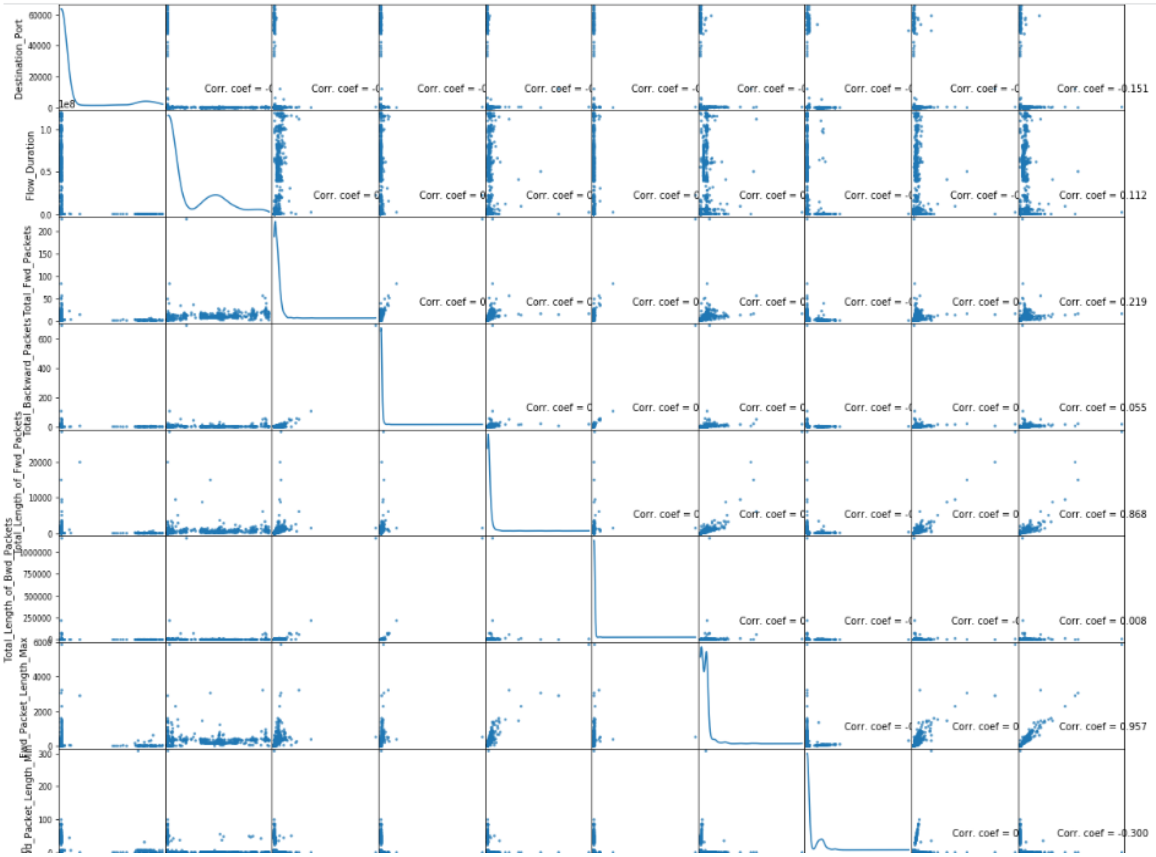

Figure 7: **Scatter Plot for the Application Layer DOS attack Dataset**

Conclusions:

Finally, this article touches on the down-to-earth cybersecurity issues that currently accompany modern supply chains, indeed, during the age of Supply Chain 4.0. When the number of supply chain attacks is increasing over time and the actors are improving their tactics, it is of great importance that the counter measures are properly developed and that fields of activity team up to master this challenge. This paper aims at analyzing the inherent vulnerabilities from the aspects of application layer protocols and network architecture and at proposing preventive measures for the risk minimization so that the organizations will ensure the security of their supply chain operations. We assume that this paper will offer a detailed guide for companies to strengthen the cyber security and secure their supply chain operations. Moreover, it shows that continuous research and the development team are necessary to get rid of the modern threats, to evolve the technologies for a changing security landscapes. With a world of augmented complexities, supply chains security, the institutions will have to adopt best practices and embrace collaboration among the stakeholders for the betterment of the system and question the legitimacy of the global networks. Lastly, by considering the views as well as proposals made in this essay, companies can improve their ability for a supply chain continuity and, therefore, they will be better placed to compete in the environment characterized with strong interconnections, digitization and innovation.

Acknowledgement:

We thank our beloved teachers whose priceless guidance and undisputed support have been indispensable in this journey of research. Through their guidance and expertise, our knowledge about Artificial Intelligence, machine learning, and blockchain technologies has been broadened. We cannot fail to thank them for their encouragement and significant contribution towards the success of our study through their critical analysis.

3. References

[1] I. Security and A. Cisa, “Defending Against Software Supply Chain Attacks,” no. April, 2021.

[2] K. Cheung, M. G. H. Bell, and J. Bhattacharjya, “Cybersecurity in logistics and supply chain management : An overview and future research directions,” *Transp. Res. Part E*, vol. 146, no. January, p. 102217, 2021, doi: 10.1016/j.tre.2020.102217.

[3] J. Hintsa, “Supply Chain Cyber Security – Potential Threats SUPPLY CHAIN CYBER SECURITY – POTENTIAL THREATS,” no. November 2018, 2013, doi: 10.11610/isij.2904.

[4] M. Nasrulddin *et al.*, “LogForum,” vol. 17, no. 1, pp. 49–57, 2021.

[5] A. Ghadge, M. Weiß, N. D. Caldwell, and R. Wilding, “Managing cyber risk in supply chains : A review and research agenda 1 Introduction,” vol. 25, no. 2, pp. 223–240, 2020, doi: 10.2139/ssrn.3426030.

[6] Jenny Chang, “97 Supply Chain Statistics You Must Know: 2023 Market Share Analysis & Data,” *FinancesOnline Reviews for Business*, 2022. https://financesonline.com/supply-chain-statistics/ (accessed Jan. 14, 2023).

[7] J. Simon and A. Omar, “Cybersecurity investments in the supply chain : Coordination and a strategic attacker,” *Eur. J. Oper. Res.*, no. xxxx, pp. 1–11, 2019, doi: 10.1016/j.ejor.2019.09.017.

[8] T. Sobb and B. Turnbull, “Supply Chain 4 . 0 : A Survey of Cyber Security Challenges , Solutions and Future Directions,” pp. 1–31, 2020, doi: 10.3390/electronics9111864.

[9] P. Threats, “Supply Chain CyberSecurity”.

[10] N. G. Filho, N. Rego, and J. Claro, “ScienceDirect ScienceDirect Supply chain flows and stocks as entry points for cyber-risks Supply chain flows and stocks as entry points for b , cyber-risks,” *Procedia Comput. Sci.*, vol. 181, no. 2020, pp. 261–268, 2021, doi: 10.1016/j.procs.2021.01.145.

[11] P. Osterrieder, L. Budde, and T. Friedli, “The smart factory as a key construct of industry 4.0: A systematic literature review,” *Int. J. Prod. Econ.*, vol. 221, 2020, doi: 10.1016/j.ijpe.2019.08.011.

[12] O. Bongomin, G. Gilibrays Ocen, E. Oyondi Nganyi, A. Musinguzi, and T. Omara, “Exponential Disruptive Technologies and the Required Skills of Industry 4.0,” *J. Eng. (United Kingdom)*, vol. 2020, 2020, doi: 10.1155/2020/4280156.

[13] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, “applied sciences IoT Privacy and Security : Challenges and Solutions,” *Appl. Sci. — Open Access J.*, vol. 10, no. 4102, pp. 1–17, 2020.

[14] S. Pandey, “Modern Network Security: Issues and Challenges,” *Int. J. Eng. Sci. Technol.*, vol. 3, no. 5, pp. 4351–4357, 2011.

[15] L. Belli, L. Davoli, A. Medioli, P. L. Marchini, and G. Ferrari, “Toward Industry 4.0 With IoT: Optimizing Business Processes in an Evolving Manufacturing Factory,” *Front. ICT*, vol. 6, no. August, pp. 1–14, 2019, doi: 10.3389/fict.2019.00017.

[16] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, “A review of iot sensing applications and challenges using RFID and wireless sensor networks,” *Sensors (Switzerland)*, vol. 20, no. 9, pp. 1–18, 2020, doi: 10.3390/s20092495.

[17] S. Raza, M. Faheem, and M. Guenes, “Industrial wireless sensor and actuator networks in industry 4.0: Exploring requirements, protocols, and challenges—A MAC survey,” *Int. J. Commun. Syst.*, vol. 32, no. 15, pp. 1–32, 2019, doi: 10.1002/dac.4074.

[18] A. Spark, “Towards Near-Real-Time Intrusion Detection for IoT Devices using Supervised Learning and Apache Spark,” 2020.

[19] N. Khalil, M. R. Abid, D. Benhaddou, and M. Gerndt, “Wireless sensors networks for Internet of Things,” *IEEE ISSNIP 2014 - 2014 IEEE 9th Int. Conf. Intell. Sensors, Sens. Networks Inf. Process. Conf. Proc.*, 2014, doi: 10.1109/ISSNIP.2014.6827681.

[20] S. O. M. Kamel and N. H. Hegazi, “A Proposed Model of IoT Security Management System Based on A study of Internet of Things (IoT) Security,” *Int. J. Sci. Eng. Res.*, vol. 9, no. 9, pp. 1227–1244, 2018, [Online]. Available: https://www.researchgate.net/profile/Samah_Kamel3/publication/328163339_A_Proposed_Model_of_IoT_Security_Management_System_Based_on_A_study_of_Internet_of_Things_IoT_Security/links/5bbc74254585159e8d8f245a/A-Proposed-Model-of-IoT-Security-Management-Syste

[21] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. Yin, “Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges,” *IEEE Access*, vol. 6, pp. 6505–6519, 2017, doi: 10.1109/ACCESS.2017.2783682.

[22] B. Mohamed and M. Abdelrehim, “Wireless Sensor Technology Selection for I4 . 0 Manufacturing Systems,” p. 109, 2020.

[23] A. Khanna and S. Kaur, *Internet of Things (IoT), Applications and Challenges: A Comprehensive Review*, vol. 114, no. 2. Springer US, 2020. doi: 10.1007/s11277-020-07446-4.

[24] L. Kirichenko, T. Radivilova, and C. Anders, “Detecting cyber threats through social network analysis: short survey,” *Socioecon. Challenges*, no. 1, pp. 20–34, 2017, doi: 10.21272/sec.2017.1-03.

[25] A. D. Jurcut, P. Ranaweera, and L. Xu, *Introduction to IoT Security* , no. December. 2020. doi: 10.1002/9781119527978.ch2.

[26] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” *Digit. Commun. Networks*, vol. 4, no. 2, pp. 118–137, 2018, doi: 10.1016/j.dcan.2017.04.003.

[27] T. C. Jesus, P. Portugal, D. G. Costa, and F. Vasques, “A comprehensive dependability model for QOM-aware industrial wsn when performing visual area coverage in occluded scenarios,” *Sensors (Switzerland)*, vol. 20, no. 22, pp. 1–22, 2020, doi: 10.3390/s20226542.

[28] K. Haseeb, I. U. Din, A. Almogren, and N. Islam, “An energy efficient and secure IoT-based WSN framework: An application to smart agriculture,” *Sensors (Switzerland)*, vol. 20, no. 7, 2020, doi: 10.3390/s20072081.

[29] D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, *Cybersecurity Issues in Wireless Sensor Networks: Current Challenges and Solutions*, no. 0123456789. Springer US, 2020. doi: 10.1007/s11277-020-07213-5.