A Security Matrix for Cyber Risks in IOT Enabled Supply Chains

Gauri Salunkhe[1], Prerna Goswami[2], Akansha Bhargava[3]

ICT, Mumbai

Abstract

With supply chain (SC) industry adopting digitization at all its stages, their ultimate objective is pointing towards features of Industry 4.0. Number of smart devices that communicate and respond to each other with IOT, allows all SC members to peep into the network to gain live updates seamlessly. This improves the transparency in business but opens doors for attackers. This paper surveys the cyber threats the IOT supply chain gets exposed to and mitigation techniques used to deal with such breaches. We propose system architecture encompassing IOT-SC with NIST cyber security framework guidelines. We formulate cyber security matrix for supply chains that lays IOT model on NIST cyber security framework.

Keywords: *IOT, Supply chains, cyber security, security matrix*

1. Introduction

Supply chain Management (SCM) involves expansive set of activities to be performed for transformation of raw entities into end products and making them available for consumers in a smooth and efficient manner. The process starts with planning, collecting resources, designing & turning them into final deliverables, and making them available at desired locations. It involves entities like suppliers, customers, factories, distributors and retailers which are interested to fulfill customer order [1]. The two most crucial among this complex set are logistics and inventory that deals with storage and transportation of goods.

However traditional supply chain management systems severally faced problems such as overstocking, delivery delays and stock out etc. These degrade the performance, increasing cost, complexity and vulnerability [2]. Due to availability of global markets supply chains span large geographical regions. Collaboration of no. of participants demands easy and clear communication (conveying requirement of raw materials, inviting tenders, allocation of orders, demand, purchase order, billing, feedback etc.) between stake holders of SC. In this era of internet and technology, participants that give faster and smarter response hold their place in business. This took SCMs towards IoT, an adept web of all smart devices that allows all its members to peep into the network to gain live updates seamlessly. To balance demand and supply ratio, predicting market conditions and for improving business decisions. Data scientists also utilize supply chain statistics that give overview of real time progress.

IOT enabled supply chains are remotely manageable, better co-ordination between the partners and availability of more accurate real time information improves decision making and customer satisfaction [3]. The sensors provide information about demands, location of goods during transport, stocking details at warehouse, delivery to customer etc. thus covering entire lifecycle of the product. It also manages geographically dispersed vendors, distributors, customers effectively.

However involvement of huge number of stakeholders and unreliability of IOT infrastructure are identified as complicated issues in supply chains when security shows up. Taking into account the maximum count of breaches carried on supply chains and cyber vulnerabilities of IOT, designing and following unified approach to identify, mitigate and monitor risks through pre defined policies requires framework or standard protocols. We try to outline security matrix, by laying IOT Model on cyber security framework defined by NIST (National Institute of Standards & technology) for supply chains.

This paper is organized as follows: section II highlights the concept of IOT based supply chain, Section III describes the cyber threats faced by IOT SC, Section IV suggests important considerations while designing security policies, and Section V introduces Security matrix.

2. Related Work

2.1 IOT enabled Supply chain

Internet of things in context of supply chain management is an active network of sensors and gateways connected digitally for sensing, monitoring and interaction to facilitate co-ordination of stakeholders of the SCM with sharing resources and information to assist them with planning, control and coordination of processes for supply chains. Mengru tu et.al.[4] highlighted upon the factors that affect enterprises' intention to adopt IoT for logistics and supply chain management. Their findings reveal that IIoT has been applied by enterprises to assist in the collection of on-site real-time information, which has successfully improved and promoted operating efficiency.
IOT make system transparent by providing clear picture of the product flow at all stages starting from manufacturer to on its way to warehouse, distributers and finally to the customer. All the items entering the SC are RFID tagged. Vehicles with active GPS modules are used to transport goods. Whenever these goods enter or leave warehouse or inventory, RFID scanners automatically reads tags and make database entry. The smart IOT devices monitor delivery process that involves inventory and order management at warehouse, and transportation. These IOT sensors can detect low stock of any product and automatically order from the manufacturers based on pending demands and previous order data. Smart active RFID tags can store information about the product or RFID reader ID, along with tag Id thus securing against tapering. RFID readers scanning tags also stores date, timestamp. System reliability is built upon safe, and on-time delivery. Data collected by sensors is stored through internet to Cloud, that provides storage, virtual resources and computing services hosted by professional networking companies (third party service providers) [5].

2.2 Cyber risks for IOT Supply Chains

With IOT connectivity, communication and interaction with other devices, platforms and shared infrastructure supply chain gets exposed to plenty of cyber threats. We discuss about major sources of cyber risks faced by IOT SC, their impact on performance and possible mitigation techniques used by researchers in the field.

Unreliability of IOT Devices: IoT devices are often made to work with low power consumption, and have limited processing capabilities so that they can monitor and sense surrounding activities with uninterrupted services. However these restrictions make them easy targets for attackers. Unreliability of IoT technology when dealing with cyber risk, is one of the major reason that industries are still not adopting ioT for supply chains [4]. Babar et.al [7] highlight in built security of IOT devices. They designed embedded security framework taking into account computational time, energy consumption and memory requirement. IOT devices from trusted designers with secure hardware, software, authentication and access control can protect the network.

Third party Involvement: Collaboration of larger groups is another big issue faced in SCM. Organizations are bound to share data, credentials, software code, applications, networks, and infrastructures with "trusted" supply chain partners. Attackers take advantage of this opportunity and take entry through loosely protected networks of SC partners. Also outsourcing of services and resources such as logistics and cloud involves third parties in the system. Increasing globalization and expansion of business underlines severity of this issue.

Data sharing and vendor processing: are the two most cyber imperative areas identified by Sharma in[8]. The open data sharing among all partners of supply chain poses challenge on information security. System databases are always been eyed by cyber criminals. Selecting cryptographic platforms, authentication and attestation are possible solutions to maintain secured central database. Involvement of vendors with their systems invites third party access.

Table below summarizes the Iot supply chain attacks. IOT attacks can be classified into five types [7] as given in the table:

Table1. IOT Supply chain attacks

Sr. No.	Type of attack	Name	Motive	Impact	Mitigation Techniques
1	Physical Attacks	Reverse Engineering	Steal information/ Gaining Access	Hackers can use the chip to gain its working knowledge	Authentication, access control, setting strong passwords
		Hardware threats [7]	Steal information	Counterfeit ICs, Hardware trojans	side-channel signal analysis, functional test, etc
		Physical tampering [11]	Theft of IoT devices	Disturbs working, interruption in data collection	Highly protected environment
2	Side Channel Attack [9]	Power Analysis	Steal information/ Gaining Access	Monitors variations in power consumption for correct & incorrect pass codes	Secrete cryptographic keys
3	Network Attack	Access/control through malicious nodes [7]	Less secure communication standards	It can gain control over every connected device and track the network	Authentication, HMAC, Access control techniques
		Cloning & spoofing [9]	To take down system	Cloned tags duplicate valid tag ids to gain access to system	secure operating systems, configuring the protocols used with the least possible privileges.
		Man-In-the-Middle [10]	To take system down	Sending spam messages/ phishing , IoT devices may reveal confidential data	keyed-hash message authentication code (HMAC) for data integrity & authentication
		Denial of service attack [11]	To take down system	Hackers create unwanted traffic to block resources	Intrusion detection systems (IDS)
		Eavesdropping [10]	Steal information/ Gaining Access	Unauthorized reader listens to streaming between tag & reader, Attackers may alter real data	Symmetric encryption algorithms such as Advanced Encryption Standard (AES)

				collected by sensors	
4	Software attack [13]	Spreading viruses	Third party involvement, stealing data	System gets spoiled	Worm detectors, Antivirus, IDS
5	Crypto analysis Attack [14]	Staling credentials of valid IoT devices	To get access to system	Hackers crack encryption keys	Lifetime credentials for devices, strong passwords

3. Research Objective

Integration of technologies certainly improves system model; however increased interdependencies among various entities, results in vulnerabilities that impose security challenges [11].The introduction of IoT technology in supply chains invites issues like managing complexities and resources efficiently [6]. This feels the need for standardization of reference architecture and cyber security framework. But the stacked IOT architecture at present lack clarification at individual layers about the strategic, functional and operational challenges from cyber community.

4. Proposed System architecture

The proposed model shown in fig.1, encompasses three fold architecture consisting of physical course of actions, E-links and Response links. Physical flow narrates steps involved in delivery of goods from SC entities (suppliers, manufacturers, vendors, distributors, customers etc.) in hierarchy from manufacturer to buyer. But this delivery is supported by IOT functions such as automatic order placing, GPS traceable logistics, scanning of products and maintenance at inventory etc. with RFID and smart networks. Technical process moves on E-inks with creation & maintenance of product scanning records, website creation and updation, cloud handling, coordination between SC partners etc. The novel Response links involve precautionary safety measures that need to be integrated for consistent performance. Continuous anomaly detection, risk assessment, suitable mitigation, responding smartly to the attacks and fast recovery with , updating security practices of network are the practices proposed for improving system architecture.

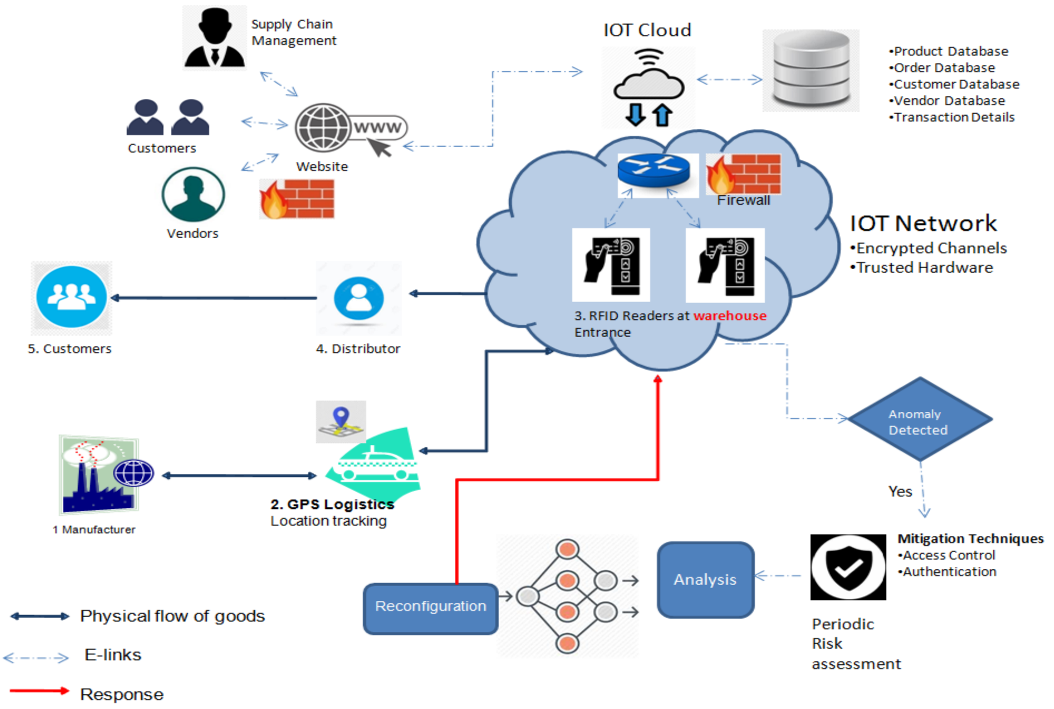


Figure 1. System Architecture

5. IOT-NIST Security Matrix

Figure 2 is collection of all cyber security enablers with protocol details. This security matrix is formulated by laying four level IOT layered architecture [15] on NIST cyber security framework [16] for IOT-SC. Researchers have came up with mitigation techniques for different attacks. However implementation of all possible solutions would result in increased overhead & reduced performance [13]. Matrix columns are numbered (1 to 5) from left to right & rows are numbered from bottom to top (1 to 4).

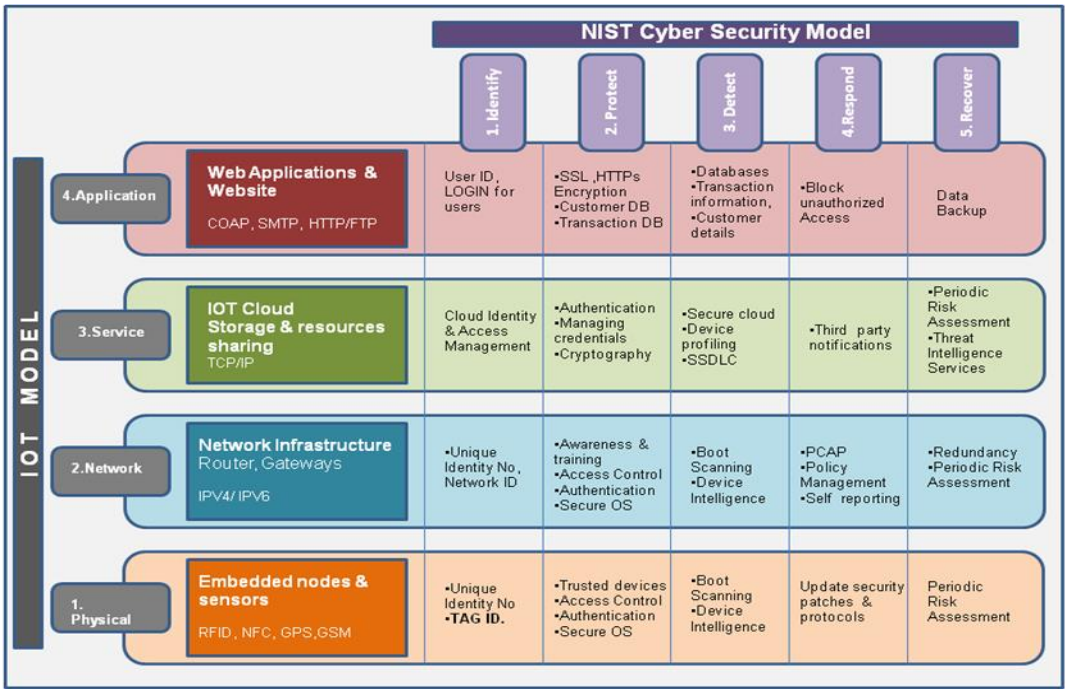
Identify: Resources available must be uniquely identifiable for risk assessments and proper governance. Endpoint devices are assigned unique identifier (TagID for RFID), network functions with unique network IDs (IP address) for devices routers, gateways etc. Cloud access & user grants are controlled with cloud Identity and Access Management (IAM). Similarly web applications and website login restricts system access & permissions.

Protect: Taking precautionary measures to safeguard resources and system elements against known threats helps to build robust architecture. Protected access, awareness and training, identity management are the activities under this phase.

Detect: This refer to developing and practicing activities to recognize and trap attempts to breach system. Anomalies and unusual activities can be automatically detected and alert can be sent if detection procedures are put in place. Cloud security can control user access and SSDLC (Secure Software Development Life Cycle) can protect software running on cloud [17].

Respond: Well defined instructions and guidelines to take actions against detected cyber events, improves ability to contain the impact of reported event. It starts with response planning, communication, analysis, and mitigation. Applying concepts such as Artificial Neural Networks or Deep Learning would improve implemented security policies, by learning from experience and updating system to mitigate newly discovered threats.

Recovery: Being ready for the emergency beforehand ensures organizations readiness to withstand critical situations. Resilience and system recovery in fastest possible manner, avoiding system collision on single node and ability to recover to normal state are expected outcomes [18].



IOT MODEL		NIST Cyber Security Model				
		1. Identify	2. Protect	3. Detect	4.Respond	5. Recover
4.Application	Web Applications & Website COAP, SMTP, HTTP/FTP	User ID, LOGIN for users	•SSL ,HTTPs Encryption •Customer DB •Transaction DB	•Databases •Transaction information, •Customer details	•Block unauthorized Access	Data Backup
3.Service	IOT Cloud Storage & resources sharing TCP/IP	Cloud Identity & Access Management	•Authentication •Managing credentials •Cryptography	•Secure cloud •Device profiling •SSDLC	•Third party notifications	•Periodic Risk Assessment •Threat Intelligence Services
2.Network	Network Infrastructure Router, Gateways IPV4/ IPV6	•Unique Identity No, Network ID	•Awareness & training •Access Control •Authentication •Secure OS	•Boot Scanning •Device Intelligence	•PCAP •Policy Management •Self reporting	•Redundancy •Periodic Risk Assessment
1. Physical	Embedded nodes & sensors RFID, NFC, GPS,GSM	•Unique Identity No •**TAG ID.**	•Trusted devices •Access Control •Authentication •Secure OS	•Boot Scanning •Device Intelligence	Update security patches & protocols	Periodic Risk Assessment

Figure 2. Proposed Security Matrix

6. Conclusion

Installing updated guidelines & security patches at all levels of system model, regular governance of resources, risk evaluation & strategic management for rectification are suggested measures in literature to deal with cyber risks for shared architectures. Regular risk assessments of SCs to update cyber security firmware are essential to raise alarm whenever high risk areas are identified. But the system would realize smart behavior in true sense if it is able to stand back at its position with minimum loss if breach is encountered. System configuration to respond to incurred situation and efforts to get recover from the attack, updating security protocols with new lesson as well as eliminating possible vulnerabilities completes the security procedure. The presented security matrix suggests techniques that take into consideration origin of threat in IOT-SC architecture; however compatibility with organizational structure must be confirmed & nature of supply chain also deserves attention.

References

[1] Supply Chain Council, “Supply chain operations reference model”, Revision 11.0, USA, (2012).

[2] M. Abdel-Basset, G. Manogaran and Mai M., “Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems”, Future Generation computer Systems., vol. 86, (2018), pp. 614-628.

[3] M. Ben-Daya, E. Hassini, and Z. Bahroun, "Internet of things and supply chain management: a literature review", International Journal of Production Research., vol. 57, no. 15-16, (2019), pp. 4719-4742.

[4] M. Tu, "An exploratory study of Internet of Things (IoT) adoption intention in logistics and supply chain management", The International Journal of Logistics Management., (2018).

[5] He Longfei, Mei Xue, and Bin Gu, "Internet-of-Things Enabled Supply Chain Planning and Coordination with Big Data Services: Certain Theoretic Implications", Journal of Management Science and Engineering., (2020).

[6] P. Radanliev, D. C. De Roure, J. RC Nurse, P. Burnap, E. Anthi, U. Ani, L. Maddox, O. Santos, and R. Montalvo, "Cyber risk from IoT technologies in the supply chain–discussion on supply chains decision support system for the digital economy",(2019).

[7] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for internet of things (IoT)", Proceedings of 2nd International Conference on Wireless Communication, vehicular technology, information theory and aerospace & electronic systems technology, Chennai, India, (2011), pp. 1-5.

[8] S. Sharma, "Cyber risks in Industry 4.0–Digital Supply Chain", CYBERNOMICS 1, vol. 5, (2019), pp.17-20.

[9] M. Aikaterini, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses", Inf Sys Front Vol.12, (2010), pp. 491-505.

[10] K. Yang, D. Forte, and M. M. Tehranipoor, "Protecting endpoint devices in IoT supply chain", Proceedings of International Conference on Computer-Aided Design (ICCAD), (IEEE 2015), pp. 351-356.

[11] E. Hodo, X. Bellekens, A. Hamilton, P.L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson, "Threat analysis of IoT networks using artificial neural network intrusion detection system", proceedings of International Symposium on Networks, Computers and Communications (ISNCC), (2016), pp. 1-6.

[12] A. Yeboah-Ofori, and S. Islam, "Cyber Security Threat Modeling for Supply Chain Organizational Environments", Future Internet, 11, vol. 3, (2019), pp.63.

[13] J. Deogirikar, and A. Vidhate, "Security attacks in IoT: A survey", Proceedings of International Conference on I-SMAC, (IEEE, 2017), pp. 32-37.

[14] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges", Proceedings of IEEE Symposium on Computers and Communication (ISCC), (IEEE, 2015) pp. 180-187.

[15] M. Burhan, R. A. Rehman, B. Khan, and B.S. Kim, "IoT elements, layered architectures and security issues: a comprehensive survey", Sensors 18, vol. 9, (2018),pp. 2796.

[16] M. Esser, "Identify, Protect, Detect, Respond and Recover: The NIST Cybersecurity Framework", (2018).

[17] AFA. Rahman, M. Daud, and M. Z. Mohamad, "Securing sensor to cloud ecosystem using internet of things (iot) security framework", Proceedings of the International Conference on Internet of things and Cloud Computing, (2006), pp. 1-5.

[18] R.H. Weber, "Internet of Things–New security and privacy challenges", Computer law & security review 26, vol. 1, (2010),pp. 23-30.