SECURED COMMUNICATION MECHANISM FOR MESSAGE AUTHENTICATION AND DATA CONFIDENTIALITY IN SECS/GEM PROTOCOL

ASHISH JAISAN S M

UNIVERSITI SAINS MALAYSIA

2024

SECURED COMMUNICATION MECHANISM FOR MESSAGE AUTHENTICATION AND DATA CONFIDENTIALITY IN SECS/GEM PROTOCOL

by

ASHISH JAISAN S M

Thesis submitted in fulfilment of the requirements
for the degree of
Master of Science

March 2024

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the following people for their invaluable contributions to my thesis work. First and foremost, I am grateful to my supervisor, Assoc. Prof. Dr. Selvakumar Manickam, for his unwavering support and guidance throughout my research journey. Your insightful comments and constructive feedback have been instrumental in shaping my work.

I would also like to extend my thanks to my co-supervisor, Dr. Shankar Karuppayah, for his continuous support, helpful suggestions, and timely feedback on my research.

My heartfelt appreciation goes to my parents for their unwavering love, support, and encouragement, which have sustained me through this challenging academic journey. I would like to acknowledge Ms. Malar Devi Kanagasabai, and the office staff, for their constant assistance and support, without which this research would not have been possible. I would like to express my gratitude to Dr. Shams Ul Arfeen Laghari, my friend, for his encouragement, valuable suggestions, and support during my studies. I am also thankful to my friend, Dr. Ayman Khallel Al-Ani, for his invaluable suggestions and support.

Lastly, I would like to thank all those who helped me during my studies. Your assistance and support have been crucial to my success, and I will always cherish your contribution to my research work. Thank you all for your invaluable contributions, support, and encouragement that have made my research work possible.

Ashish Jaisan S M, Penang, Malaysia, 2023.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

AE	Authenticated Encryption
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AI	Artificial Intelligence
ASCII	American Standard Code for Information Interchange
CoAP	Constrained Application Protocol
CPS	Cyber-Physical Systems
DDS	Data Distribution Service
EEF	Engineering Employers' Federation
GCM	Galois/Counter Mode
GEM	Generic Equipment Model
GF	Galois Field
HSMS	High-Speed SECS Message Services
IBM	International Business Machines
IDE	Integrated Development Environment
IIoT	Industrial IoT
IoT	Internet of Things
IP	Intellectual Property
IT	Information Technology
Kbps	Kilobits per second
M2M	Machine-to-Machine
MQTT	Message Queuing Telemetry Transport
NIST	National Institute of Standards and Technology
OPC UA	Open Platform Communications Unified Architecture
OSI	Open Systems Interconnection
OT	Operational Technology
PLC	Programmable Logical Controller
RFC	Request For Comments
SECS	Semiconductor Equipment Communication Standard
SECS-I	SEMI Equipment Communications Standard, Part 1
SECS-II	SEMI Equipment Communications Standard, Part 2

SEMI	Semiconductor Equipment and Material International
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TSMC	Taiwan Semiconductor Manufacturing Company
VoIP	Voice over IP
VPN	Virtual Private Network
WFH	Work From Home

LIST OF APPENDICES

MEKANISME KOMUNIKASI TERSELAMAT UNTUK PENGESAHAN MESEJ DAN KERAHSIAAN DATA DALAM PROTOKOL SECS/GEM

ABSTRAK

Industri 4.0 telah membawa revolusi dalam sektor pembuatan, yang telah menyebabkan peningkatan ketara dalam proses pembuatan dan peningkatan dalam kualiti dan kapasiti pengeluaran. Protokol komunikasi Mesin-ke-Mesin (M2M) telah dibangunkan untuk membolehkan mesin berkomunikasi dalam ekosistem perindustrian. Protokol komunikasi M2M iaitu Piawaian Komunikasi Perkakasan Semikonduktor/Model Peralatan Generik (SECS/GEM) telah wujud dalam industri pembuatan untuk tempoh yang agak lama, berfungsi sebagai protokol komunikasi dan sistem kawalan. Walaupun penggunaannya meluas, SECS/GEM tidak mempunyai ciri keselamatan seperti pengesahan mesej dan kerahsiaan, kerana ia direka untuk digunakan dalam rangkaian tertutup. Ketiadaan komponen keselamatan dalam protokol ini boleh membenarkan penggodam mencuri maklumat sulit, seperti proses pembuatan, dengan memeriksa parameter dan resipi peralatan. Mereka juga mungkin mengganggu atau mensabotaj komunikasi SECS/GEM, yang boleh memberi kesan buruk kepada industri yang menggunakan protokol tersebut dalam persekitaran mereka. Penyelidikan ini mencadangkan SECS/GEM-AE, iaitu suatu mekanisme untuk melindungi mesej data SECS/GEM dengan menggunakan penyulitan AES-GCM, dan menilai prestasi penggunaannya dalam protokol SECS/GEM asal serta SECS/GEMsec, mekanisme keselamatan yang telah dicadangkan untuk mengesahkan mesej SECS/GEM. SECS/GEM-AE berjaya memastikan kerahsiaan dan ketulenan data, dengan overhed yang amat rendah dan boleh diabaikan iaitu 0.45 milisaat dan 0.58 milisaat apabila menghantar dan menerima mesej, berbanding protokol asal.

Dalam perbandingan dengan SECS/GEMsec pula, SECS/GEM-AE menunjukkan pengurangan sebanyak 18.13 milisaat untuk menghantar mesej manakala 19.75 milisaat untuk menerima mesej. Kesimpulannya, SECS/GEM-AE adalah mekanisme yang dapat meningkatkan keselamatan untuk komunikasi SECS/GEM tanpa overhed yang tinggi.

SECURED COMMUNICATION MECHANISM FOR MESSAGE AUTHENTICATION AND DATA CONFIDENTIALITY IN SECS/GEM PROTOCOL

ABSTRACT

Industry 4.0 has brought about a revolution in the manufacturing sector, resulting in significant enhancements in the manufacturing process and an increase in production quality and capacity. Machine-to-Machine (M2M) communication protocols have been developed to bind the industrial ecosystem, enabling machines to communicate. The Semiconductor Equipment Communication Standard/Generic Equipment Model (SECS/GEM) M2M communication protocol has been at the forefront of the manufacturing industry for years, serving as both a communication protocol and control system. However, despite its widespread adoption, SECS/GEM lacks security features such as message authentication and confidentiality, as it was designed for use in closed networks. The deficiencies in the protocol can permit malevolent actors to steal confidential information, such as manufacturing processes, by examining the equipment parameters and recipes. These individuals may also disrupt or sabotage SECS/GEM communications, resulting in grave consequences for the industry. This study proposes SECS/GEM-AE, a mechanism for securing SECS/GEM data messages using AES-GCM encryption and evaluates its performance against the standard SECS/GEM protocol and SECS/GEMsec, a security mechanism proposed to authenticate SECS/GEM messages. SECS/GEM-AE successfully provides message authentication and confidentiality, with a negligible overhead of 0.45 milliseconds and 0.58 milliseconds when sending and receiving messages, respectively, compared to the standard protocol. When compared to SECS/GEMsec,

SECS/GEM-AE shows a reduction of 18.13 milliseconds in sending messages and 19.75 milliseconds in receiving messages. The results conclude that SECS/GEM-AE is the appropriate security mechanism to secure SECS/GEM communications.

CHAPTER 1

INTRODUCTION

This chapter is divided into nine sections. Section 1.1 presents an overview of Industry 4.0, its history, and the significance of Machine-to-Machine (M2M) communication protocols in modern industrial networks. Section 1.2 provides an overview of the SEMI Equipment Communications Standard/Generic Equipment Model (SECS/GEM) M2M communication protocol. Section 1.3 introduces industrial networks and the cybersecurity threats in modern industrial networks. Section 1.4 presents the motivation for this research. Sections 1.5 through 1.9 present the problem statement, research objectives, scope and limitations, research contribution, and research steps. Finally, Section 1.10 provides the organization of the rest of this thesis.

1.1 Overview

The First Industrial Revolution was the era in the 18th century when Europe, America, and Great Britain adopted novel industrial practices (Lu, 2017; Sanchez et al., 2020). This transition encompassed the transfer from manual handcrafting to machine production, the establishment of innovative iron and chemical production practices, the increased utilization of hydropower and steam engines, industrial machinery, and the factory system (Mourtzis et al., 2022). Nevertheless, industrialization in the 18th century resulted in an astonishing acceleration of production expansion. The advent of electrical technology in the mid-nineteenth century led to significant scientific breakthroughs and standardization, which echoed the objective of mass production; hence, it was termed the Second Industrial Revolution (Suleiman et al., 2022). The industries took off once the Programmable Logical Controller (PLC) was invented in late 1960, revolutionizing industrial

automation and coining the phrase Third Industrial Revolution (Alay, 2023). The rapid progression of technology in recent decades has led to the emergence of Industry 4.0, also known as the Fourth Industrial Revolution. This is due to the integration of various cutting-edge technologies such as machine learning, Artificial Intelligence (AI), robotics, Internet of Things (IoT), 5G networks, cloud computing, 3D printing, and quantum computing (Alhayani et al., 2023).

The manufacturing industry has been revolutionized by Industry 4.0, vastly improving the manufacturing process and increasing production quality and capacity. M2M communication protocols were developed to strengthen and bind this ecosystem by allowing machines to communicate with each other (Leang & Rasiah, 2023). With sophisticated machinery and automation, more integrated M2M communication, real-time monitoring and data collection, machine learning, and enhanced interconnectivity, Industry 4.0 is changing the existing manufacturing process for better and improved overall production (Zheng et al., 2021). Interconnected machines generate activity information, predictive diagnostic data, performance statistics, and other monitoring and control information. Thus, real-time decisions can be made quickly with advantages such as time and cost-saving. In many scenarios, human involvement in the factory environment can be eliminated. With the utilization of pre-set and tested settings and parameters, factory equipment can make critical decisions autonomously, thereby ensuring optimal cost-effectiveness for the industry.

M2M communication is a critical component of Industry 4.0, enabling the creation of smart factories and a more connected, automated, and efficient industrial landscape. M2M communication protocols allow machines to exchange data and control information in real-time, enabling them to operate independently and integrate

seamlessly with the factory environment. M2M communication enables machines to process and act on data, make informed decisions, and take autonomous actions to improve productivity and efficiency. M2M communication lies at the heart of Industry 4.0, which possesses the potential to revolutionize the production of goods and services by streamlining manufacturing processes and reducing the requirement for manual intervention. In addition, using M2M communication protocols can help companies gain a competitive advantage by enabling them to respond to changes in market demands and customer needs with greater agility and flexibility.

Industry 4.0 involves a lot of M2M communications and processing of sensitive data, and security is a critical concern that must be addressed to fully realize its potential. The increased data density associated with Industry 4.0, along with the convergence of information technology (IT) and operational technology (OT), brings new challenges, particularly in the area of cybersecurity (Ervural & Ervural, 2018). Cybersecurity is a top priority for governments worldwide, as it involves protecting digital business information and valuable subject or system knowledge against abuse, unauthorized access, and theft (Buch et al., 2017). Figure 1.1 presents the percentage of extortion cases per industry, due to cybersecurity incidents in 2022, observed by IBM X-Force (Worley et al., 2023) . It is reported that attacks on the manufacturing sector have significantly increased which has made manufacturing industry to lead the list.

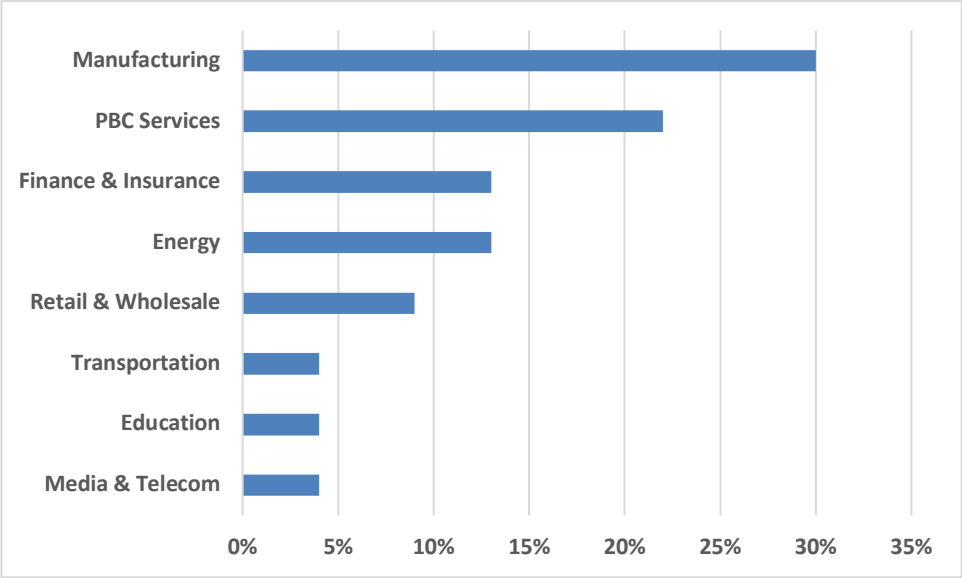

Figure 1.1 Extortion Cases Observed by IBM X-Force in 2022 (IBM, 2022)

With expanding network connections, cyberattacks have become more prevalent due to the rising tendency to misuse data for different purposes, such as financial and strategic reasons (Ervural & Ervural, 2018). Therefore it is essential to implement robust security features to avoid various cyber-attacks (Kwon et al., 2020).

The industry utilizes various M2M communication protocols, including SECS/GEM, Data Distribution Service (DDS), Open Platform Communications Unified Architecture (OPC UA), and Message Queuing Telemetry Transport (MQTT), which are among the most commonly employed protocols. Figure 1.2 shows popular IoT and Industrial IoT (IIoT) Protocols.

In the realm of the Internet of Things (IoT) and Industrial Internet of Things (IIoT), various protocols play pivotal roles in facilitating communication and data exchange between connected devices. In the domain of IoT, protocols such as XAMP, LwM2M (Lightweight M2M), and CoAP (Constrained Application Protocol) are commonly employed. XAMP provides a robust framework for real-time data streaming, while LwM2M is designed for efficient device management and CoAP, a

lightweight protocol, is optimal for resource-constrained devices. In the IIoT landscape, protocols like OPC UA (Unified Architecture), AMQP (Advanced Message Queuing Protocol), DDS (Data Distribution Service), and SECS/GEM (SEMI Equipment Communications Standard/Generic Equipment Model) take precedence. OPC UA ensures interoperability in industrial automation, AMQP facilitates efficient message queuing, DDS supports real-time data distribution, and SECS/GEM is vital in semiconductor manufacturing. Bridging the domains of IoT and IIoT, protocols such as Zigbee and MQTT find application. Zigbee is prominent in low-power, short-range communication, while MQTT is widely adopted for lightweight and efficient messaging in both industrial and general IoT scenarios. These protocols collectively contribute to the seamless integration and functionality of connected devices across diverse applications in the IoT and IIoT ecosystems.

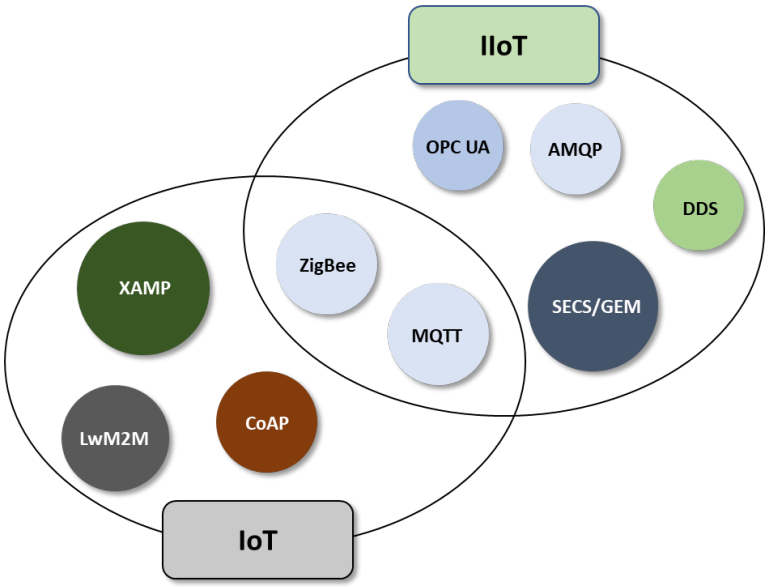

Figure 1.2 IoT and IIoT Communication Protocols

1.2 SECS/GEM Protocol – An overview

SEMI (formerly Semiconductor Equipment and Materials International) has introduced numerous standards, including four major protocol standards for

equipment-to-host communications (Ehm et al., 2020). These standards were first released in 1978, with the latest revision published in 2020. Though the SECS/GEM communication protocols were published several years ago, they are regularly maintained and updated. This section is an overview of the major SECS/GEM protocol releases. Table 1.1 gives a brief description of SECS/GEM standards.

Table 1.1 SECS/GEM Standards

Year	Standard	Description
1978	E4 SECS-I	SEMI Equipment Communications Standard-I is a communication protocol for establishing communication between equipment and a host via RS-232 cable at the physical layer of the network stack.
1982	E5 SECS-II	SEMI Equipment Communications Standard-II enables the exchange of information between equipment and hosts using streams and function messages in a defined format.
1992	E30 GEM	The Generic Equipment Model defines SECS-II message usage and monitors equipment behavior during message exchange with the host.
1994	E37 HSMS	High-Speed SECS Message Service is a protocol for managing point-to-point communication between equipment and hosts over TCP/IP.

The SECS/GEM protocol is a point-to-point M2M communication protocol, meaning factory equipment is connected to a single host machine and only communicates with the mentioned host machine. Host systems are connected to various equipment that must be SECS compliant (i.e., based on SECS standards). Serial (RS-232) or TCP/IP ports can be used to connect to the host. The GEM standard is used in some of the more recent equipment. Generally, older equipment is not GEM compliant, relying on serial connectivity. The HSMS standard operates

similarly to TCP but does not support multiple connections. A piece of equipment can only connect to and communicate with one host at a time and must disconnect from the current host before communicating with another. Figure 1.3 illustrates an implementation architecture for a SECS/GEM-enabled factory system.

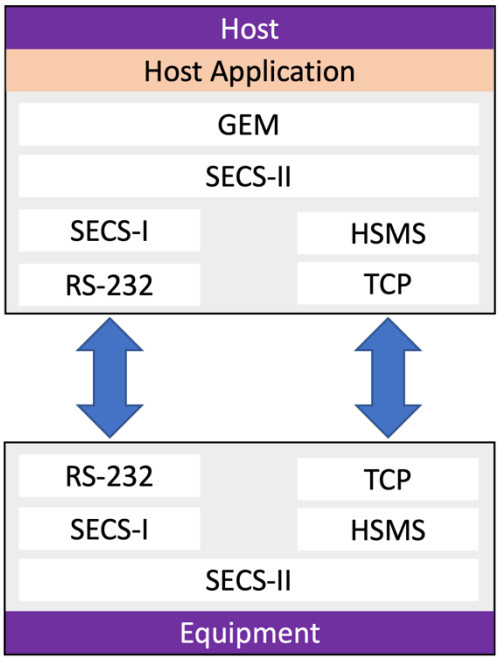

Figure 1.3 Implementation Architecture for SECS/GEM (Azaiez et al., 2019)

The host system's primary function is to manage connectivity to a group of equipment via a configuration file, recipe management, load balancing, monitoring of the equipment, and connection to enterprise-level applications. SECS/GEM messages are sent as requests and responses. For example, a host may request a piece of equipment for data, and the equipment will reply with the requested data as a response. A request message and a response message together are called a transaction. Every message has a detailed header that states the message type and its function. The SECS/GEM message structure is covered in more detail in Chapter 2.

Although SECS/GEM has been widely adopted (Ewe et al., 2020; Zhu et al., 2021), the standard does not offer any security mechanism to secure communications.

The SECS/GEM communications are transmitted as binary encoded data. An attacker with fair knowledge of SECS/GEM and binary encoding can easily read the contents of these messages. This can lead to serious problems such as intellectual property (IP) theft. Moreover, SECS/GEM does not authenticate or verify the messages' integrity and will accept and process illegitimate or modified messages. This vulnerability allows attackers to manipulate equipment with very minimal effort.

Despite the widespread use of the SECS/GEM protocol in industrial networks, little research has been conducted on securing these communications. Specifically, no work has been published to address confidentiality issues in SECS/GEM, which raises significant concerns about the security of this widely used protocol. This lack of attention has prompted researchers to develop alternative methods for securing SECS/GEM communications, such as the digital signature-based approach known as SECS/GEMsec (S. U. A. Laghari, Manickam, Al-Ani, et al., 2021a). While SECS/GEMsec offers message authentication, it fails to address other important aspects, such as data confidentiality and performance. SECS/GEMsec is covered in detail in Chapter 2.

1.3 Industrial Networks and Cybersecurity Threats

Industry 4.0 emphasizes the use of automation and remotely controllable operations. In the past, manufacturing environments were not connected to external networks, so ensuring cybersecurity was not a major concern. However, protocols were not secured even when the equipment was connected, as manufacturing networks were typically closed and air-gapped environments where external actors posed little to no threat. The drive of automation and Cyber-Physical Systems (CPS) in the manufacturing environment requires the manufacturing network to be open, therefore

requiring the evaluation of those protocols being used and addressing any forthcoming issues, especially from a security perspective.

Cyberattacks pose threats to the basic cybersecurity principles, i.e., confidentiality, integrity and availability (Brar & Kumar Ahuja, 2018). When evaluating protocols for use in Industry 4.0 environment, these cybersecurity principles are required to be followed. Figure 1.4 depicts a taxonomy of cyberattacks on cybersecurity principles (Brar & Kumar Ahuja, 2018). Attacks on cybersecurity principles (confidentiality, integrity, and availability) pose a major threat to cybersecurity. Therefore, these principles must be ensured for a secure Industry 4.0 enabled manufacturing environment.

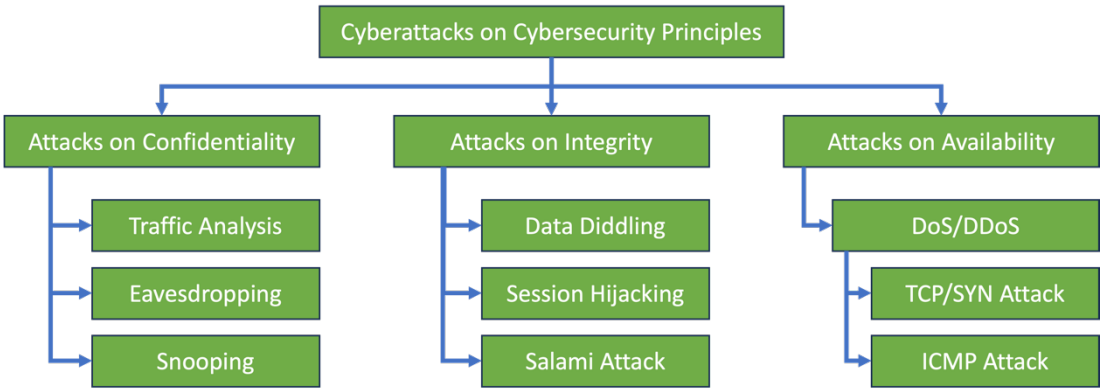

Figure 1.4 Taxonomy of Cyberattacks on Cybersecurity Principles

The manufacturing industry has been gradually updating and improving its IT security over the years; however, it can be seen in the Verizon Data Breach Investigation Report 2019 (Widup, 2019), detailing 352 cyberattack incidents, out of which 87 were against the manufacturing industry. Recent attacks and security breaches against the manufacturing industry are alarming, making it a highly targeted and vulnerable entity for attackers (Tuptuk & Hailes, 2018). A survey by the Engineering Employers' Federation (EEF) shows that 60% of manufacturers were victims of cyberattacks at some point, and one-third of the affected manufacturers have

suffered financial and market losses due to these cyberattacks. According to a study conducted by Cybersecurity Ventures in 2021, corporations across the globe are expected to experience annual losses of up to $10.5 trillion by 2025 due to cyberattacks. This projection is a significant increase from the estimated losses of $3 trillion in 2015 (Morgan, 2021). The cyberattack on Taiwan Semiconductor Manufacturing Company (TSMC) was, in Taiwan's history, the worst data security infringement to befall them. It completely exposed data security vulnerabilities at TSMC's production foundries. These cyber-attack incidents are happening as the manufacturing industry embraces the shift to Industry 4.0, with more and more machines becoming connected for communications and automation (Peng, 2018). Figure 1.5 depicts the distribution of cyber-attacks across leading industries worldwide in 2022 (Worley et al., 2023). It can be seen that the manufacturing industry suffered the greatest number of cyber-attacks and is expected to grow even further in the future.

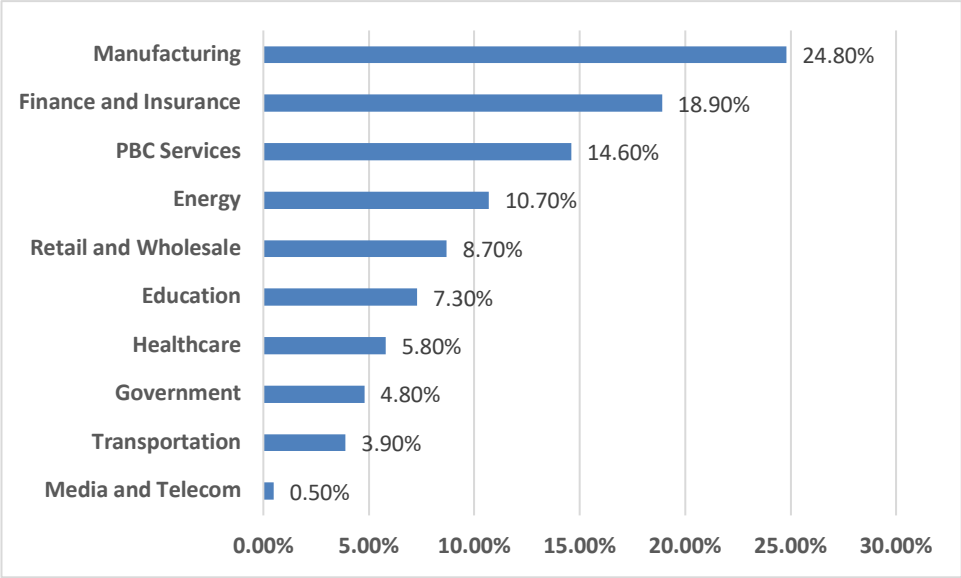

Figure 1.5 Cyber-Attacks on Industrial Sectors in 2022 (Worley et al., 2023)

At the end of 2019, the Corona Virus Disease 2019 (COVID-19) pandemic took the world by storm (Georgiadou et al., 2022). The process to stop the spread of the pandemic came with its consequences, requiring governments to impose

lockdowns and suspend operations in sectors that were deemed non-essential. The manufacturing industry came under these restrictions as well. The stakeholders had no choice but to allow their employees to work remotely and only have minimal staff to ensure their safety. This led to the Work From Home (WFH) scenario allowing employees to connect to corporate and manufacturing networks and work from home (Georgiadou et al., 2022). This scenario opened the door for cybercriminals to infiltrate manufacturing industries even from outside manufacturing facilities, rendering them vulnerable to even more cyber threats.

The cybercriminals knew of the WFH situation and only needed to break into an employee's computer to access manufacturing networks (Khatri et al., 2023). Thus in 2020, when many industries relied on their remote workers, cybercriminals took advantage of the situation to intensify their attacks. The manufacturing industry jumped from the eighth to the second most targeted industry by cybercriminals, with a 300 percent increase in cyber-attacks in a year (Kazu & Thomas, 2021).

1.4 Research Motivation

Industrial networks are increasingly vulnerable to attacks that target business secrets and intellectual property. This issue is particularly pressing in the semiconductor industry, where the SECS/GEM protocol is widely used for communication between equipment and manufacturing control systems. However, the plaintext nature of this protocol renders it susceptible to passive attacks. Since existing security mechanisms are not suitable for addressing these vulnerabilities, and if they are available, they tend to be complex and require excessive processing time for messages. Consequently, there is a crucial need for a security mechanism that can protect business secrets and maintain confidentiality in real-time. This mechanism

must also operate at high efficiency to avoid slowing down the system and impeding productivity.

Given the rapid growth of the semiconductor industry, it is essential to develop a robust and reliable security mechanism that can prevent attacks and safeguard sensitive information. By addressing the security flaws of the SECS/GEM protocol, businesses can continue to operate with the necessary confidence and security. Therefore, this research endeavors to propose a security mechanism that is not only fast and efficient but also provides real-time insights into the system, ensuring the confidentiality and protection of business secrets.

1.5 Problem Statement

Industry 4.0 has revolutionized the manufacturing industry and improved the manufacturing process, increasing quality and yield (Mourtzis et al., 2022). The same applies to the semiconductor industry, with the usage of automated machinery, robotics, sensors, and computers improving the overall production rate while, at the same time, being less prone to flaws and defects as the human element is removed and replaced with high precision machinery (Coronado et al., 2022). The whole manufacturing line of machinery, robotics, and sensors are interconnected by computers controlling everything, adjusting machine parameters accordingly, providing necessary recipes when needed, and so on (Soori et al., 2023). The operations are carried out through M2M communications, typically between a centrally managed server and the equipment and sensors. Such communication is carried out through special communication protocols. SECS/GEM is a popular M2M communication protocol widely adopted in the semiconductor industry (S. A. Laghari, Manickam, Karuppayah, et al., 2021). Although SECS/GEM has been widely adopted,

the standard does not offer any security mechanism to secure communications (Al-Shareeda et al., 2022). Researchers have proposed security mechanisms for SECS/GEM communications; however, they prove inadequate to be used in a production environment as they do not address necessary security vulnerabilities in SECS/GEM.

The SECS/GEM protocol and existing works on security features for SECS/GEM suffer from the following key issues:

The SECS/GEM standards and existing works exchange data in plaintext which makes it vulnerable to intellectual property theft. The existing works incur that offer security for SECS/GEM protocol are compute-intensive and require significant processing time, thus rendering their applicability unsuitable for the real-world applications.

1.6 Research Objectives

The objectives of this research are to achieve the following:

1. To propose a security mechanism that provides message authentication and data integrity.
2. To propose a security mechanism that provides data confidentiality.
3. To propose a security mechanism with minimal overhead and high efficiency to provide performance close to the standard SECS/GEM.

1.7 Scope and Limitation

The scope of this thesis is limited to proposing a security mechanism for authenticating industrial devices communicating over SECS/GEM protocol and

providing data confidentiality to the information exchanged between the two devices over the industrial communication network. Table 1.2 summarizes the overall research scope for the proposed security mechanism.

Table 1.2 Research Scope

Item	Scope of Research
Environment	TCP/IP Network
Security Mode	Authentication, Confidentiality
OSI Target Layer	Application Layer, Transport Layer
Evaluation Metrics	Processing Time, Protocol Control Overhead

This research employs symmetric key encryption algorithms. The secret keys employed in the encryption process are stored locally on the communication entities. The distribution and secure storage of secret keys are beyond the scope of this study.

1.8 Research Contribution

SECS/GEM is one of the most powerful and widely implemented protocols in the manufacturing industry, yet its security features have only recently been realized. The current research focuses only on authentication and prevention of cyberattacks to enable using this protocol in the Industry 4.0 ecosystem. Hence, this study focuses on the authentication and confidentiality of SECS/GEM with a focus on performance. The forthcoming study is expected to make the following contributions:

1. The proposed mechanism enables SECS/GEM devices to encrypt communications, attain data confidentiality and prevent Intellectual Property (IP) theft.

2. The proposed mechanism secures SECS/GEM communications while maintaining performance acceptable in a production environment.
3. A testbed environment is developed to evaluate the performance of the proposed mechanism in terms of processing time and control overhead.

1.9 Research Steps

It is convenient to split the research into five stages or steps to attain this study's objectives. These phases are as follows: problem identification, literature review, research methodology, implementation, and evaluation. Figure 1.6 illustrates each of these stages/steps and associated activities to complete this study.

Step 1: Problem Identification. This stage covers the SECS/GEM communication protocol in general and delves deeper into the underlying SEMI communication standards to highlight the SECS/GEM protocol's strengths and weaknesses. Security threats to SECS/GEM communications caused by a lack of confidentiality support are also identified at this stage. The problem statement is defined based on the issues identified. The scope and limitations are established in this stage as well.

Step 2: Literature Review. This stage reviews existing security solutions available for SECS/GEM. Hence, this stage provides deeper insight into the limitations of existing solutions and the requisite knowledge to describe the proposed solution.

Step 3: Research Methodology. This stage describes the proposed mechanism with authentication and confidentiality features for SECS/GEM communications. The proposed mechanism must not change the existing SECS/GEM message structure. It

must also be efficient for encrypting and authenticating messages while maintaining acceptable performance.

Step 4: Implementation. This stage explains the specifics of how the proposed mechanism is implemented, the programming language, and the steps taken to execute the proposed mechanism in the testbed environment. Additionally, this phase discusses software tools for monitoring and capturing network traffic. The tools discussed will be used in conjunction with the development of the proposed mechanism. Additionally, a testbed will be developed to examine the functioning and efficiency of the proposed mechanism. The proposed mechanism is executed, and its performance is evaluated in various configuration modes.

Step 5: Evaluation. This stage is the analysis of the experiment results. The results are evaluated based on certain evaluation matrices and compared with existing works. The proposed mechanism is also evaluated to verify if all the objectives were attained. Future works and improvements for the proposed mechanism are also identified.

Figure 1.6 Research Steps

1.10 Thesis Organization

This thesis is organized into six chapters.

Chapter 1 introduces Industry 4.0 and the semiconductor manufacturing industry. An overview of M2M communication protocols and SECS/GEM M2M

communication protocol is also presented. The problem statement, research objectives, and research contributions are also established in this chapter.

Chapter 2 provides a background on SECS/GEM standards and cybersecurity issues associated with its protocols. It also reviews existing security mechanisms for SECS/GEM, their features, and shortcomings. It also reviews existing techniques that may be used to secure SECS/GEM communications.

Chapter 3 presents the methodology of this research work, detailing the features and requirements. It also proposes the design of a testbed to experiment with the proposed mechanism.

Chapter 4 presents the implementation of this research work, the programming language used, and the monitoring tools used. It also explains, in detail, the experiments, including variations and scenarios used in the experiments.

Chapter 5 presents the results, compares the results with existing works based on certain evaluation matrices, and discusses the findings of this research.

Chapter 6 summarizes this research work, provides suggestions for future work, and concludes this thesis.

CHAPTER 2

LITERATURE REVIEW

In this chapter, Section 2.1 presents a brief discussion of the SEMI organization and the manufacturing industry. Section 2.2 provides a comprehensive background of SEMI's SECS/GEM standards, namely SECS-I, SECS-II, HSMS, and GEM (also known as E4, E5, E37, and E30, respectively). The security issues of SECS/GEM are discussed in Section 2.3. Section 2.4 covers encryption and various types of encryption algorithms. In addition, this chapter reviews existing SECS/GEM communications security solutions and highlights their limitations in Section 2.5. The chapter is summarized in Section 2.6.

2.1 Background

SEMI is a global conglomerate of companies that focus on the semiconductor industry, comprising members worldwide. The organization consists of 26 subgroups: Manufacturing, Packaging & Test, Automated Test Equipment, Market Statistics, Information & Control, Health & Safety, and more (Goh et al., 2017). SEMI provides equipment, software, materials, and services to produce electronic devices, such as semiconductors, flat panel displays, photovoltaic cells, and other products (SEMI, 2020). Their market research provides valuable information on trends and advancements in semiconductors and related industries, encompassing market size, growth rates, and technological innovations. SEMI also aims to establish industry standards in the manufacturing, testing, and electronics supply chain to create universal guidelines. Additionally, SEMI supports policies and regulations that promote the growth and competitiveness of the semiconductor industry and others.

The utilization of automation in the semiconductor manufacturing industry has been gaining importance in recent times. Technologies such as robots, AI, and computer vision are being deployed to boost efficiency, cut costs, and improve the quality of products. According to recent studies, automation technologies in semiconductor industry can lower manufacturing costs while decreasing production time (Mane, 2022). Additionally, automation is helping to minimize environmental pollution, as automated systems can more accurately supervise and regulate semiconductor production processes. Furthermore, automation technologies could decrease waste and improve product quality (Javaid et al., 2021).

Figure 2.1 depicts simplified equipment configurations within an industrial production line network.

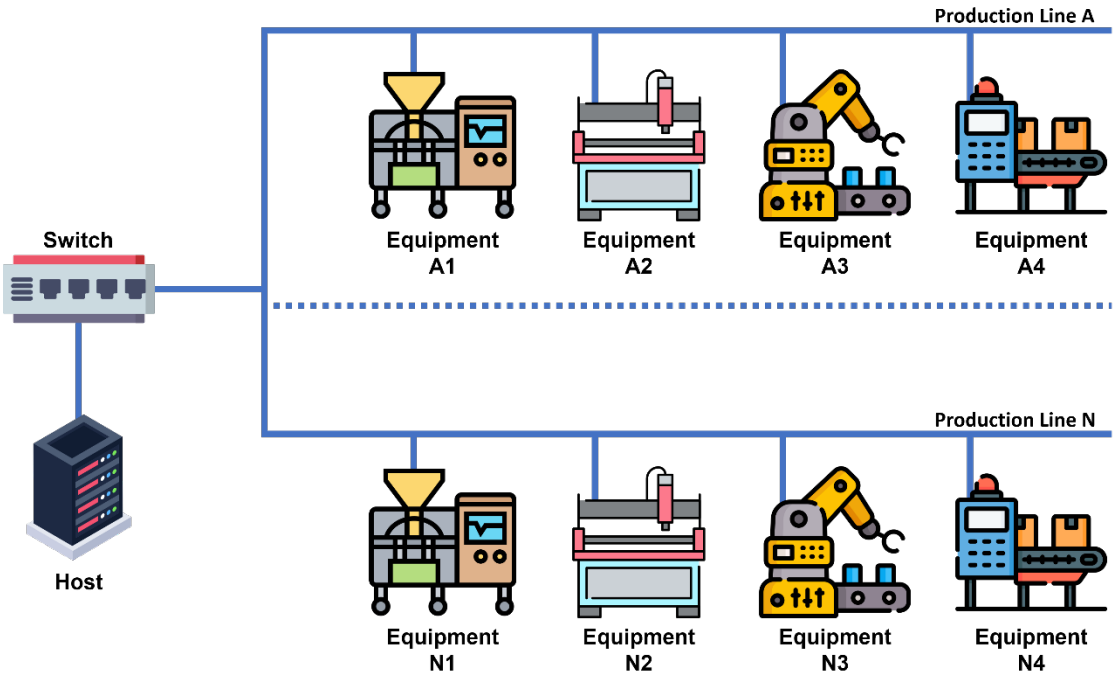

Figure 2.1 Simplified Industrial Production Network Topology

M2M communication has become a critical component in industrial networks, where numerous devices, sensors, and machines need to interact and share information to enable automation and optimize production processes. M2M communication allows machines to communicate with each other directly without human intervention,

reducing the need for manual monitoring and control. This type of communication can occur over various protocols. By leveraging M2M communication, industrial networks can achieve greater efficiency, accuracy, and speed, reducing costs and increasing productivity. Additionally, M2M communication can enable predictive maintenance and real-time monitoring of industrial assets, improving reliability and reducing downtime. In numerous cases, there will be no involvement of human intermediaries. Instead, machines can independently make critical decisions with predetermined and controlled parameters, thus optimizing cost-effectiveness for the manufacturer. The SECS/GEM communication protocol is discussed in this chapter based on relevant scientific research.

2.2 SEMI M2M Communication Standards

Semiconductor Equipment and Material International (SEMI) is a global association with over two thousand members that provides equipment, materials, and services to the manufacturing industry. It has created several standards, including E4, E5, E30, and E37, to facilitate communication between factory equipment and the host. These standards are collectively known as SECS/GEM, as shown in Table 1.1. The hierarchal representation of SECS/GEM standards are shown in Figure 2.2. SECS/GEM is an industry-standard used in various manufacturing industries for decades. In companies such as Intel, Samsung, TSMC, IBM, Qualcomm, Broadcom, UMC, SK Hynix, Micron, TXN, Toshiba, NXP, and others, SECS/GEM serves as a communication protocol and control system, making it an essential part of the semiconductor industry for many years.

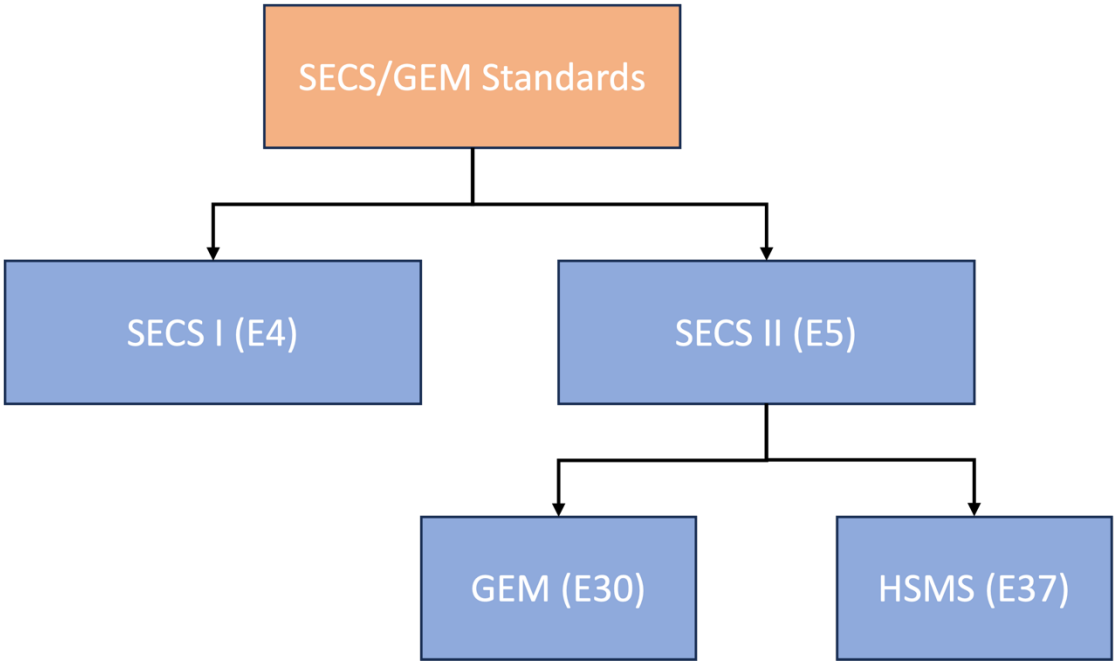

Figure 2.2 SECS/GEM Standards Hierarchal Representation

The SECS/GEM standard establishes a set of requirements for communication between semiconductor manufacturing equipment and host computer systems. SECS/GEM protocol defines a set of features referred to as *Fundamental Requirements* that equipment suppliers must implement in their devices to ensure compatibility with other equipment and host systems. Fundamental requirements are the basic features that are mandatory for all SECS/GEM-compliant devices, including status report messages, data collection, and event reporting. Following is the detailed list of fundamental requirements of SECS/GEM standard:

- Message structure: The SECS/GEM standard defines a specific message format that should be used for communication between equipment and host systems. This message structure includes fields for message type, equipment ID, transaction ID, and data.
- Message transfer protocol: The standard defines a protocol for transferring messages between equipment and host systems. This protocol includes

procedures for establishing and terminating communication sessions, sending and receiving messages, and error handling.

- State model: The SECS/GEM standard defines a state model for equipment that specifies the various states that equipment can be in during manufacturing. This state model provides a common language for equipment and host systems to communicate about the status of equipment.
- Alarms and events: The standard defines a set of alarm and event messages that can be used to notify host systems of equipment status changes or errors. These messages can trigger automated responses or alert operators to take corrective action.
- Data collection: The SECS/GEM standard defines a set of data collection messages that can be used to request specific information from equipment or to send data to equipment for processing.

The SECS/GEM standard provides a standardized framework for communication between semiconductor manufacturing equipment and host computer systems, which helps to ensure interoperability and compatibility between different systems.

In addition to the fundamental GEM requirements, SECS/GEM interface can support several optional capabilities depending on the specific implementation and requirements of the equipment and host systems involved. Some of the optional capabilities that a GEM interface can support include the following:

- Remote Command and Control: This allows the host system to send instructions to the equipment and carry out operations remotely.
- Recipe management: This capability enables the host system to manage the equipment's recipes for every manufacturing process.

- Traceability: This capability enables the equipment to provide data about the manufacturing process that can be used to trace products through the production processes.
- Data monitoring: This capability enables the host system to collect and monitor data from the equipment to analyze performance, identify trends, and make informed decisions.
- Dynamic allocation of resources: This capability enables the equipment to adjust its resource allocation based on real-time data and conditions to improve efficiency and optimize performance.
- Automatic material handling: This capability enables the equipment to handle and process materials used in manufacturing automatically, thus, reducing the need for manual intervention and increasing productivity.

The optional capabilities supported by a GEM interface depend on the specific needs and requirements of the equipment and host systems involved and can vary widely depending on the implementation.

2.2.1 SEMI Equipment Communications Standard 1 (SECS-I)

SEMI E4 standard, or SECS-I, is a communication protocol used in the semiconductor industry to enable communication between equipment and factory control systems. The SECS-I standard defines the physical and electrical interface for data transfer between devices, including message transmission, data structures, and message sequences. This standard is based on RS-232 serial communication protocol and operates at a speed of up to 57.6 kilobits per second (kbps). SEMI developed SECS-I to standardize communication protocols in the industry, improve equipment efficiency, and reduce downtime. Despite its speed and data capacity limitations, SECS-I remains an important standard in the semiconductor industry, particularly for older