International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

# Technology Innovations Model of Artificial Intelligence to Stop Industrial Espionage in Manufacturing Establishments

**Biswaranjan Senapati[* 1], Bharat S Rawal [2] , Awad Bin Naeem[3] ,Prasanna Chandran Melnatami Krishnaram [3] ,Sunilkumar Guduru[4] , Sachin Sharma[5] , Prasenjit Banerjee[6], Sudhakar Tiwari[7]**

**Submitted**: 27/01/2024 **Revised**: 05/03/2024 **Accepted**: 13/03/2024

***Abstract:*** In the digital age and at smart manufacturing sites, the production units have been facing a lot of challenges concerning industrial espionage and are vulnerable, critical, and under a growing threat that needs cybersecurity practices, policies, and cryptography in place. Most manufacturing firms have been facing the biggest challenge, as they have been facing critical issues concerning security, confidentiality, availability, and accessibility of the confidential manufacturing process, formulas, and core research and development credentials. In the United States, there have been a high number of cybersecurity data breach and industrial espionage cases reported, with manufacturing and other industries being the most heavily affected; of the 1579 data breach cases reported, 620 were related to manufacturing. Most industrial sites must protect their intellectual property and maintain confidentiality while also securing operational and manufacturing transactions across multiple sites. Key critical data, day-to-day operational master data, corporate key data, and data governances, as well as formulas, key production compositions, and valuable intellectual property (IP), are stored in secure locations and accessible to authorized users in the organization. However, there have been a few cases of data theft by hackers and other people who shouldn't have access to it on real-world systems, as this could happen due to access to virtual reality. This could include potential risks and critical losses to industrial manufacturing segments that must bear the loss of business due to an inability to meet global trade compliance requirements, as well as data losses at the enterprise level. In operational planning, industrial espionage is one of the most critical cases that could potentially harm the reputation of individual manufacturing sectors and render them unable to fulfill customer orders (MTS or MTO). Several major cases of industrial espionage and trade secret theft have been reported and published in academic journals. In 2012, the NSA director and commander of US Cyber Command reported that industrial espionage and cyber espionage exclusive to industrial manufacturing sites could result in a loss of $ 338 billion per year, which is a significant amount of money and data. Some technology innovations models (AI, ML, and quantum computing, ERP-SAP, and Zero-trust) AI, ML, or quantum cyber security models could potentially save data and prevent IP and other credentials from being stolen, as well as update the robust security and cybersecurity platform to protect against potential industrial espionage or future threats within the manufacturing sites. Most industrial manufacturing sites, such as defense production, airship production, pharmaceuticals, or even a high-tech manufacturing company where technologies and innovations are crucial to performance, see intellectual property (IP) as the most important and valuable thing that needs to be secured and protected. Only authorized employees or vendors should be able to access IP, and an audit and log trial should be kept. Per KPMG research studies, industrial espionage could be easily targeted concerning accessing back-office systems, like ERP, production control systems, manufacturing execution, and inventory databases, to steal the critical product formulas and credentials to manage to copy the most sensitive trade secrets, which could be potential IE.

***Keywords:*** *Industrial Espionage, AI, Quantum Computing, Manufacturing, and ERP-SAP HANA Zero trusts*

## 1. Introduction

Most industrial applications and business operations in the smart factory model within Industry 4.0 are controlled by intelligent equipment, back-office enterprise resource planning (ERP) applications like Oracle or SAP S/4 HANA, and other technology-dependent devices like sensors. However, there is an elevated level of vulnerability and security challenges concerning application software or even front-end applications of manufacturing sites [1-2]. Management of smart factories is handled by industrial control systems (ICS) and IIoTs, including day-to-day operational activities through big industrial data and applications systems (PLC & SCADA) that are core application systems. These threats cause production systems to shut down and pose various challenges to industrial efficiencies to fulfill the "make to production order" or "make to stock" scenarios. As per the recent reviews by [3-5], Industry 4.0 applications cost a considerable amount and are increasing significantly estimated to reach $232 billion (B) by 2024 [6-7]. Most manufacturing production sites may use advanced artificial intelligence and machine learning tools and large ERP back office and front-end applications with a connection interface to front-end customer-facing tools [8]. Analysts forecast an increase from 237 million (M) in 2016 to 950 million in the next five years. When it comes to digital innovations, there are a few hurdles and

*[1] Capitol Tech University, Department of CS, Maryland, USA*
*ORCID ID: 0000-0002-0717-5888*
*[2] Capitol Tech University, Department of CS, Maryland, USA*
*ORCID ID: 0000-0001-8808-6280.*
*[3]Department of Computer Science, NCB&E, Multan, Pakistan.*
*ORCID ID: /0000-0002-1634-7653*
*Corresponding Author Email: bsenapati@ualr.edu*

critical factors to consider. Reported issues in cybersecurity and cryptography have associated risk factors [9]. A recent survey shows that manufacturing and industrial sites are the most vulnerable and attacked industries regarding their physical and information security compliance status [10]. Smart factories, devices, and high-end digital industrial sites are subject to highly vulnerable attacks such as exploitation, cybercrime, industrial spies, malware, denial of service (DoS), and hacking [11]. Managing cyber-attacks and taking preventive measures while dealing with the assailant is challenging. The United States is home to several essential organizations tasked with cyber security, being the most well-known for releasing many cyber security reports and recommendations (e.g., 800-82 guide) [12]. Nations or states, terrorist organizations, corporate spies, cybercriminal organizations, "hacktivists," and hackers are all identified threats. It also cites a third party [13] that distinguishes between thrill-seekers and insiders as a third group of actors.

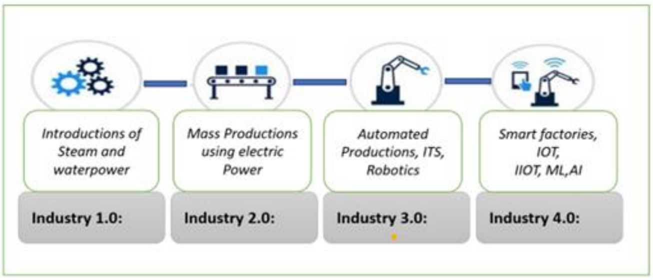

Introductions of Steam and waterpower
Mass Productions using electric Power
Automated Productions, ITS, Robotics
Smart factories, IOT, IIOT, ML,AI
Industry 1.0:
Industry 2.0:
Industry 3.0:
Industry 4.0:

**Fig. 1.** Industrial Revolutions and Useful of Technologies

### 1.1 Industrial Espionage and Best Global Manufacturing Practices (GMP):

Industrial espionage at manufacturing sites is widespread and dangerous because of the demand for unethical user access to production facilities via virtual environments, websites, or even the Internet of Everything (IoE). The best endpoint connections, devices, sensors, and central industrial ERP systems are essential for ensuring global manufacturing practice (GMP) compliance in manufacturing. Productive outcomes from smart factories require that the sites prioritize best practices in cyber security, industrial cryptography, and industrial espionage. In a broad sense, industrial espionage refers to the unethical practice of stealing industrial business trade secrets from company A or company B using spies and hackers to gain a competitive advantage. Governments use this more for commercial and business purposes than for national security. Managing industrial espionage at significant production facilities presents a few difficulties, including data loss and decreased productivity. There are substantial obstacles to overcome when thinking about data security and the prevention of industrial espionage at manufacturing facilities. As per industrial manufacturing, the good manufacturing practices (GMP) system ensures that manufactured goods, like heavy industrial products, food, cosmetics, and pharmaceuticals, are consistently produced and controlled according to set quality standards. These are all achieved by utilizing processes, procedures, and documentation. Furthermore, its goal is the reduction of manufacturing losses and waste, as well as the risk of recall, seizure, fines, and even goodwill from the customer and suppliers [13- 14]. Per the best practice of GMP compliance, both the business and the customer are safeguarded against unfavorable food safety events and quality production at the sites. Cross-contamination, adulteration, and mislabelling are just a few potential disasters that can be avoided with good manufacturing practices (GMPs). Stated are some of the principal challenges of industrial espionage while thinking about industrial applications:

- High amount of unethical, illegal practices behavior in industrial and enterprise data breaches.
- Steal a business's trade secrets and handed for business
- Data Leakage, security breach Problems with internal employees, current applications, and core
- Sox compliance, financial audits, audit logs, and a lack of cybersecurity training and practices in organizational practices.
- Authentication, authorization, and accessibility should be given to the right users for the right access to systems and process areas.

### 1.2 Critical components of goods manufacturing practices (GMP) in manufacturing sites:

The use of public and private cloud services has transformed contemporary enterprise networks into a hybrid environment, in contrast to the past when business organizations ran out of their own or hosted data centers. Organizations have embraced different cloud service models (IaaS, PaaS, and SaaS). Hosted data centers, multi-cloud services, and on-premises resources are all combined to form a typical IT infrastructure. Through software-defined networking and public internet access, cloud resources and services operate in a hyperscale environment. Secure network channels across the Internet or specialized private connectivity that is natively offered by Hyperscale services further enable this. The lines between business networks have become hazier with this hybrid approach. The networks have gotten more diverse, and uniform policy enforcement and decision points are needed to secure the landscape across a wide range of platforms. Security automation and software-defined networking ought to make this possible. The nature of threats is changing, and attacks are becoming more complex. This is coming from both the organization's exterior and its mobile workforce, which is spread everywhere. Regardless of where it is being accessed, the "zero-trust" architecture framework substantially aids in the security of all data flows, identities, applications, and endpoints.

A good manufacturing practice consists of five components critical to managing the best productivity in production sites, potentially saving manufacturing sites from cyber-attacks and industrial espionage. Adhering to and practicing Good Manufacturing Practices (GMP) in the workplace is crucial for manufacturers to guarantee reliable product quality and safety. The following 5Ps of good manufacturing practice (GMP) are essential for ensuring that rigorous regulations are met at every manufacturing stage (Fig. 2).

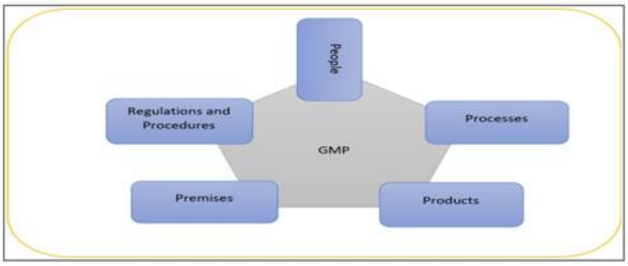


**Fig. 2.** Good Manufacturing Practices

- **People.** In manufacturing sites, all workers must religiously follow the production procedures and rules. All employees must complete up-to-date GMP training to understand their roles and responsibilities fully.
- **Products.** Per the GMP practices, manufacturers and employees should ensure that only the highest quality goods reach the market. They must be tested, compared, and rated repeatedly. Primary materials like natural products and other components should have detailed specifications at each manufacturing stage.
- **Procedures.** It should be well-defined, well-defined, and well-distributed to all staff members. To guarantee that all workers are following the established procedures and achieving the necessary levels of performance, it is necessary to conduct regular evaluations.
- **Premises:** Maintaining a clean environment is essential for preventing disease transmission, injuries, and even deaths. To reduce the possibility of equipment failure, it's important to calibrate and maintain all machinery regularly to make sure it's ready to deliver reliable results every time.

The following is a list of a few industrial espionage cases (Fig. 3) we have seen in industrial manufacturing sites that are extremely vulnerable and costly to deal with in terms of competitive advantages.

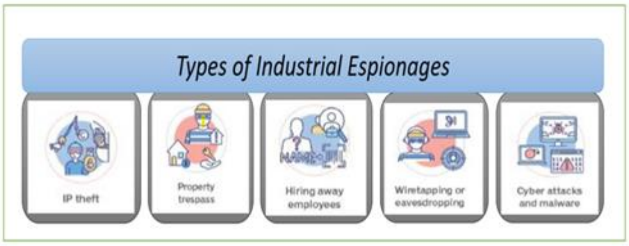

Types of Industrial Espionages
IP theft
Property trespass
Hiring away employees
Wiretapping or eavesdropping
Cyber attacks and malware

**Fig. 3.** Types of Industrial Espionage

## 2 Related Works

Corporate sabotage could be an attractive choice in situations with multiple competitors. The target is usually a significant rival to tarnish their name. This can be done in several ways, including paying criminals to use their DDoS infrastructure to take down a website or system or launching malicious cyber-attacks designed to steal information. It can be used against the targeted business by exposing sensitive or embarrassing information to the public. Despite the widespread illegality of cyber operations, some legal gray areas remain where businesses can operate (see Fig. 4 for an illustration of this idea). Non-commercial entities, such as political campaigns, also qualify as competitors. To give just one recent example, cyber operations impacted the outcome of 2016. U.S. presidential election. Some publicly employed legal tactics (like cybersquatting) may not be ethical or even legal in some countries [14-18]. The equivalent retaliation theory, or strategy, from game theory, addresses this web of ideas. This research aims to establish criteria for identifying hostile acts between actors based on their prior relationship. If two parties used to work together, but one has done something to harm the other, the injured party will look for a chance to retaliate in kind. When a political party's policy negatively impacts one of its members, it can lead to a breakdown in trust between the two parties. Then, in the future, the party member could take the same precautions and reclaim his losses. Similar parallels can be drawn between competing corporations in that, just as one firm may cross a legal threshold to harm another, the latter may cross the threshold to retaliate against the former. The risk of being discovered is the primary harm to companies thinking about engaging in offensive cyber operations. Unfortunately, nations have proven the efficacy of plausible deniability online [19-22].

### 2.1 Cyber Attack and Cause of Industrial Espionage

Cyber-attacks are episodes on computer systems, networks, and devices that hackers or other malicious actors carry out to steal sensitive information, spread malware, disrupt services, or cause harm. These attacks can take many forms, including phishing scams, malware infections, denial-of-service attacks, and more. Cyber-attacks can have severe consequences for individuals, businesses, and governments, as they can lead to the loss of sensitive data, monetary loss, damage to reputation, and even physical harm in some cases. Others may be motivated by a desire to cause harm or gain notoriety and engage in cyber vandalism or cyber terrorism. Still, others may be motivated by a desire to test their skills or expose systems vulnerabilities to improve security.

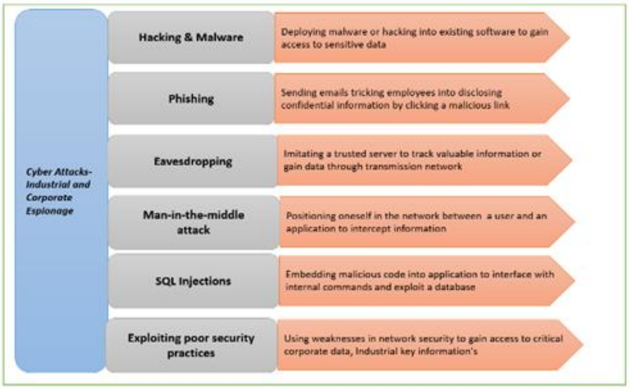

Cyber Attacks- Industrial and Corporate Espionage
Hacking & Malware
Deploying malware or hacking into existing software to gain access to sensitive data
Phishing
Sending emails tricking employees into disclosing confidential information by clicking a malicious link
Eavesdropping
Imitating a trusted server to track valuable information or gain data through transmission network
Man-in-the-middle attack
Positioning oneself in the network between a user and an application to intercept information
SQL Injections
Embedding malicious code into application to interface with internal commands and exploit a database
Exploiting poor security practices
Using weaknesses in network security to gain access to critical corporate data, Industrial key information's

**Fig. 4.** Methods of Industrial and Corporate Espionage

### 2.2 Cyber-Physical System

Cyber-physical systems (CPS) are networks of cooperative computational entities that are intricately linked to the physical environment and its ongoing activities. They access and use Internet-based data processing and retrieval services simultaneously. Put differently, a computer and communication core are responsible for monitoring, controlling, coordinating, and integrating the functions of "physical and engineered systems." The interplay between the physical and the cyber parts is crucial. Separate comprehension of the computational and physical components is insufficient. Their relationship is something we need to comprehend. The CPS has tremendous potential to transform many facets of existence. Intelligent buildings, robotic surgery, driverless automobiles, smart energy grids, smart manufacturing, and implanted medical devices are just a few of the use cases that have already surfaced [22-23]. Industrial Hyperphysical Systems Requirements are essential and indispensable for production management in industrial manufacturing systems. The Industrial Internet of Things and CPS will have a big effect on manufacturing enterprises. IoT and CPS principles are now used across most businesses, yet there are few applications in the manufacturing sector. Limited research has been conducted in other industries involving embedded sensors in the production of RFID-tagged items. Data collected from these devices undergo minimal data analysis. The IoT data may be analyzed using these technologies, and the results can then be utilized to inform decisions. Figure 6 illustrates the many ways in which cyber-physical manufacturing systems outperform traditional manufacturing systems.

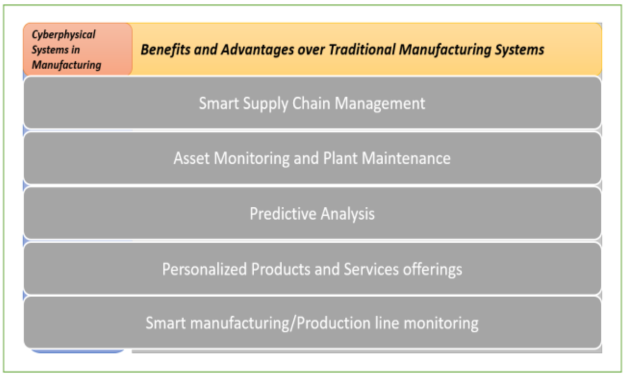

Cyberphysical Systems in Manufacturing
Benefits and Advantages over Traditional Manufacturing Systems
Smart Supply Chain Management
Asset Monitoring and Plant Maintenance
Predictive Analysis
Personalized Products and Services offerings
Smart manufacturing/Production line monitoring

**Fig. 5.** Usability of CBS in manufacturing sites

### 3 Possible Solutions using AI and ML

Through assisting in the detection, prevention, and response to cyber threats, artificial intelligence has the potential to greatly enhance cyber security. AI may be used in the following ways to strengthen cyber security:

1. Threat detection: Large volumes of data may be analyzed by AI algorithms, which can then spot trends and abnormalities that might point to a cyber threat. AI, for instance, may be used to spot malware, recognize phishing emails, and spot odd login habits.

2. Prevention: AI can be used to predict and prevent cyberattacks by identifying and blocking potential threats before they can do damage. For example, AI can be used to identify and block malicious websites or prevent the spread of malware.

3. Response: AI can automate cyber threat response, giving businesses the ability to react to assaults swiftly and successfully. It enhances overall security by being able to recognize, neutralize, and recover from cyber threats. AI is not a cure-all, however, since it depends on training data, is subject to prejudice and mistakes, may be costly, and needs constant upkeep. AI-based cybersecurity solutions may also be costly and need constant updating. When using AI in cyber security, ethical considerations including possible exploitation or misuse must be considered. As a result, businesses should use prudence when using AI and take into account its dangers and limits.

### 3.1 Pattern Recognition

To enable zero defect production, higher quality goods, and increased customer satisfaction, time-series analytics is currently being effectively used for pattern recognition applications in the manufacturing sector. Machine learning algorithms are used in pattern recognition, a data analysis technique that automatically finds patterns and regularities in data. Below phases of Pattern Identification are much required in manufacturing practices. A subfield of machine learning called pattern recognition places special emphasis on identifying patterns in data. It is divided into two main sections.

- The goal of exploratory pattern recognition is to find broad patterns in data. The algorithms concentrate on searching the data for obscure patterns or feature clusters. Their primary method is unsupervised classification, which designates an unknown class for the input pattern.
- The goal of descriptive pattern recognition is to classify the patterns that have been found and place them into a predetermined class. Supervised categorization is mostly used.

A classification or categorization job frequently involves pattern recognition. In supervised classification, the classes are established by the system; in unsupervised classification, the classifications are learned based on pattern similarity. Different Models for Pattern Recognition are listed in this paper: The primary methods for pattern recognition identify the many kinds of models that are frequently employed. Figure 8 shows three types of pattern recognition. models.

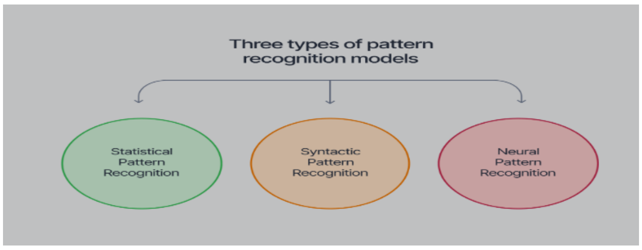

Three types of pattern recognition models
Statistical Pattern Recognition
Syntactic Pattern Recognition
Neural Pattern Recognition

**Fig. 6.** Three types of pattern recognition models

### 3.2 Predictive Analysis

The method of utilizing data to project future results is known as predictive analytics. To identify patterns that could indicate future behavior, the method makes use of statistical models, machine learning, artificial intelligence, and data analysis. The benefits of predictive analysis in manufacturing sites are in huge demand. It is the fundamental technological approach that underpins predictive maintenance, and several other industrial applications is predictive analytics. In addition to various applications of this technology, we shall examine predictive maintenance analytics here: Predictive maintenance is one of the key applications of predictive analytics, as previously indicated. In predictive maintenance, manufacturing equipment performance data points (like temperature and vibration) are recorded by industrial sensors, uploaded in real-time, and analyzed using analytics modeling to find small performance variations that might be early warning signs of more serious potential maintenance issues. Then, well in advance of equipment faults or shutdowns, these problems may be proactively resolved. Moreover, predictive maintenance addresses the following domains.

- Ordering and managing inventory with a better understanding and precision of part requirements and usage.
- Saving time and money through more focused and efficient maintenance troubleshooting made possible by root cause analysis.
- Predictive asset maintenance analytics, developing more focused maintenance procedures to increase the lifespan of machines and components.
- Utilizing more extensive analytical modeling, risk analysis extends beyond the immediate identification of preventive maintenance problems to provide well-informed evaluations of high-risk regions that could need unplanned repair.
- Predictive analytics, or macro forecasts, may also be helpful outside of the shop in situations like supply chain management and inventory demand forecasting. For instance, procuring raw materials for manufacturing may be one of the most erratic and hence expensive resource expenditures in production. The market's whims, which are influenced by a plethora of uncontrollable and hard-to-assess elements, might have an impact on sourcing.
- In the manufacturing business, human management continues to be the most crucial and valuable resource. It is a well-known fact, nevertheless, that managing people in the industrial setting is harder than it has ever been because of shifting demands, challenges in filling and maintaining open positions, and the daily demands of often challenging duties. With predictive analytics managing everything from traditional HR assistance to data-centric employee engagement and performance monitoring, all these areas may be enhanced while a more productive staff is created.

Ultimately bringing some clarity to a long-opaque process, predictive analytics uses vast volumes of historical data to make sense of previous patterns and future likelihoods. Similar strategies are used in demand forecasting analytics, which may also leverage technology like machine learning (ML) to further increase its predicted accuracy.

### 3.3 Benefits of Predictive Analytics in Manufacturing

Now that we are aware of the potential applications of predictive analytics, let's examine the advantages they may provide: Increased equipment uptime: In the industrial industry, time is money. Unplanned equipment outages have a major detrimental effect on project performance indicators and the company's bottom line, interfering with work schedules, deadlines, and balance sheets. Much more control over equipment uptime and downtime is possible with predictive maintenance, which makes it possible to schedule repairs for periods when it will have the least impact on output. Improved inventory control: Because there always seems to be too much or too little of a certain item on hand, inventory is one of the production process' most wasteful areas. More informed inventory decisions and orders can be made thanks to predictive analytics, which also makes just-in-time planning easier and produces more precise inventory management than before. Increased command over variables that appear uncontrollable: Predictive analytics may provide far better-informed decision-making, even while nobody can, of course, forecast the future. Predictive analytics may offer a more thorough and useful perspective of impending possible risk factors, opportunities, and suggestions in a variety of domains, including demand forecasting, inventory management, supply chain, and more, by utilizing big-data strategies and models.

### 3.4 Post Quantum Cryptography

Post-quantum cryptography, or quantum encryption, is the field of study concerned with creating cryptographic systems for classical computers that are resistant to assaults by quantum computers. During the 1980s, researchers hypothesized that computers could outperform binary, classical computers in complex calculations if they could leverage the special capabilities of quantum physics. The utilization of quantum features like superposition and entanglement allowed a quantum computer to do complicated computations in a matter of hours, which would have taken years for a traditional computer. This was evident very early. In the 1990s, cryptographers worldwide started investigating the possible architecture of a post-quantum cryptography system following mathematician Peter Shor's famous demonstration that a theoretical quantum computer might break the public key encryption (PKE) technique with ease. Standards for post-quantum encryption are still being developed as of this writing. Using the concepts of quantum physics, quantum computers process data in qubits more quickly than traditional computers. Pre-quantum cryptography employs an algorithm to translate readable input into secret code, but it has trouble creating ciphers that are both straightforward and difficult to crack. Quantum cryptography creates unbreakable secret codes by using the physical properties of atoms and geometric ciphers. Post-quantum cryptography has many challenges, too, including the relatively new science of quantum physics and the enormous expense of developing and operating quantum computer prototypes.

### 3.5 The Post-Quantum Cryptography of The Future

Public-key cryptography and other encryption techniques are thought to be secure enough for use in e-commerce. Quantum computing is a genuine technology, but it is costly, and its applications are limited to government and scientific research. Researchers are racing against each other to discover a practical post-quantum encryption method as well as to use quantum algorithms to crack cryptosystems like RSA. Many scientists predict that in nine or ten years, quantum supremacy will be achieved, making RSA and other asymmetrical algorithms ineffective in protecting sensitive data. That's why NIST is working hard to develop a post-quantum encryption specification. While NIST is busy assessing the viability of proposed standards for post-quantum cryptography, experts advise organizations to use the next few years to track third-party and public encryption libraries and to compile a reference index for applications that use encryption. The index can be used to create a plan for updating or replacing apps that employ cryptography after post-quantum cryptography implementation techniques have been developed and a standard has been adopted. It is important to distinguish between quantum key distribution (QKD) and post-quantum cryptography. Key interception may be readily identified when two distant parties share a secret cryptographic key thanks to QKD.

### 3.6 Threats to the Manufacturing Sector Presented by Quantum Computing

Potential risks to IT infrastructure security are a key worry associated with the use of quantum computing in manufacturing. Never forget that present conventional computers are far inferior in power to quantum computers. To properly encrypt data and issue and validate digital identities to users, devices, and applications, modern computers employ cryptographic methods. Nowadays, RSA, ECC, or DSA are among the often-used methods. The issue is that a quantum computer may launch a cyberattack on these methods, breaking practically all asymmetric encryption protocols now in use. Consequently, there's a good chance that internet data is exposed to PQC attacks and is not safeguarded. NIST is in the process of replacing the existing data protection methods and algorithms with new ones, known as Post Quantum Cryptography (PQC), to prevent cyberattacks. These algorithmic and protocol improvements should significantly lower the likelihood of cyber breaches by individuals looking to employ quantum computing for malicious purposes rather than for legitimate purposes. The development of CRQC (Cryptographically Relevant Quantum Computers) faces danger from another source that directly targets businesses. Currently, a technique known as "steal now decrypt later" is being used by hackers to gather encrypted data to employ a quantum computer to decode it later. Next, hackers could target the systems of the manufacturer to steal confidential information, and intellectual property, or even interrupt operations.

### 3.7 Automated Response System

#### 3.7.1 Auto-Encoders

These are a type of artificial neural network that can be used for dimensionality reduction, feature learning, and anomaly detection. In the context of cyber security, autoencoders can be used to detect anomalies in network traffic, such as malware or malicious activity. To do this, an autoencoder is trained on a dataset of normal network traffic. When the autoencoder is then presented with new network traffic, it can use its learned representation of normal traffic to identify anomalies in the new traffic. They are especially useful for detecting anomalies in large and complex datasets because they can learn to identify subtle patterns in the data that a human might miss, however, it is important to note that auto encoders can be vulnerable to bias and errors, and they require ongoing training and maintenance to remain effective.

#### 3.7.2 K-Means Algorithm

These algorithms belong to a class of clustering algorithms that are useful for organizing data points into clusters according to how similar they are. K-means algorithms may be used to cluster network traffic data in the context of cyber security. A K-means algorithm must first be trained on a dataset of typical network traffic to be used for this purpose. Each data point is assigned to the cluster with the closest mean, or "centroid," after the algorithm splits the data into a predetermined number of clusters. When the K-means algorithm is then presented with new network traffic data, it can use its learned representation of normal traffic to identify data points that do not belong to any of the clusters, which may indicate an anomaly or cyber threat. K-means algorithms can be useful for identifying patterns and anomalies in large and complex datasets, but they can be sensitive to the initial placement of the centroids and may not always produce the best results. Additionally, K-means algorithms are not well-suited for data with non-linear patterns or outliers, and they can be vulnerable to bias and errors.

#### 3.7.3 Graph Neural Network

Graph neural networks are a specific kind of artificial neural network that can be applied to the analysis and processing of data in graph form. For cyber security, GNNs can examine data on network traffic to spot any unusual behavior that might point to an attack. Since networks can be represented as graphs—with nodes representing devices or servers and edges representing connections between them—GNNs can be especially helpful when analyzing network traffic data. To detect anomalies or suspicious activity, GNNs can be trained to recognize patterns in the graph structure and node attributes. Furthermore, GNNs can be applied to the analysis of data from other sources, such as social media or email, within the realm of cyber security. There are many potential applications for GNNs in cybersecurity, including the detection of suspicious communication or behavior patterns that could indicate an attack. Even though GNNs have the potential to be an effective tool for detecting cyber threats, they can be difficult to design and train and necessitate substantial amounts of data. When applying GNNs to cyber security, it’s crucial to think about their limitations and drawbacks.

### 3.8 Zero-trust and Industrial manufacturing sites

There is a growing need for the Internet of Things and industrial Internet of Things in manufacturing production sites and smart manufacturing practices. These technologies are valuable in many ways, but they also bring with them several security issues. Security is sometimes included after the fact as an add-on rather than as a crucial component that is incorporated from the beginning of a product's lifetime, even though intricate manufacturing supply networks give hackers several ways to breach a gadget. In real-world industrial manufacturing, we can't be as sure that components like hardware, firmware, and credentials haven't been tampered with by the more supply chain partners in the production process. Because their supply chains are so intricate, all manufacturers—especially those that make Internet of Things (IoT) devices—need to adopt a "zero trust" approach to security. By combining public key infrastructure, hardware-based security, embedded security, key and certificate lifecycle management, device trustworthiness, code signing, and authentication, zero-trust manufacturing aims to produce dependable products via an unreliable supply chain. By 2026, the electronic manufacturing services (EMS) industry is projected to have grown from $500 billion in 2019. With this strategy, security vulnerabilities are more likely to occur, and OEMs may swiftly expand contract manufacturing to companies throughout the EMS industry, giving them a competitive advantage via reduced production risks, accelerated time-to-market, and competitive prices.

### 3.9 Common Security Concerns Simply Emphasize the Need for Zero Trust Manufacturing

Going deeper, zero-trust manufacturing is even more necessary in light of several prevalent security issues, particularly for IoT manufacturers. Many of the worst cyberattacks and security breaches that affect manufacturers involve sophisticated methods to get security credentials. The Verizon 2020 Data Breach Investigation Report states that hacking accounted for 45% of breaches, and that brute force or the use of credentials that had been obtained was used in 80% of those breaches. These assaults, which directly impact enterprises, are usually the result of stolen user and device credentials, including digital certificates and private keys. 92% of firms had at least one certificate-related outage in the previous 24 months, and 81% reported numerous disruptive disruptions because of expired certificates, according to a Poniman Institute study supported by Key Factor. Therefore, safeguarding devices and apps against sophisticated attacks across the supply chain requires controlling and securing private keys and digital certificates using a zero-trust strategy. The following are a few of the most prevalent IoT dangers and weaknesses that a zero-trust strategy may assist defend against.

- Man-in-the-middle attacks: A type of cyberattack when hackers assume the identity of a user and change data by using credentials they have obtained.
- Root CA impersonation is an attack wherein hackers compromise the root Certificate Authority (CA).
- Unauthorized firmware upgrades are the result of a hacker-infected code signing credential breach.
- Intellectual property theft and counterfeiting refer to cyberattacks wherein hackers use stolen credentials to pilfer intellectual property and introduce fake goods onto the market.

## 4. Connected Worker and Trust-Zero at Manufacturing Sites

Industrial organizations are reaping several benefits from having a connected workforce. However, the corresponding hazards necessitate more sophisticated, zero-trust cybersecurity systems. Prominent industrial enterprises use ubiquitous, round-the-clock accessibility to systems, applications, data, and personnel to propel increased efficiency, superior caliber, and reduced expenses. Despite the significant advantages, there are also more cyber hazards. Each encounter creates a fresh avenue for assault. Additionally, there are more chances for malware infection and data loss while using devices outside of facilities. The industrial cybersecurity programs that are in place now were not created to handle these threats. To safely make use of all the advantages of connectivity, businesses must adopt zero trust security. Every industry activity is seeing greater performance thanks to connected personnel. Travel expenses and facility downtime are being decreased by employees who have remote access to resources and systems. Construction delays and expensive mistakes are being decreased by site staff who have immediate access to project information. Factory workers' productivity is increasing due to their instant access to cloud resources and subject matter experts. Travel expenses and safety concerns are being decreased by the remote operation of equipment in remote and dangerous places. Utilizing productivity-boosting technology like cloud analytics, smart eyewear, and augmented reality more widely is made possible by connectivity.

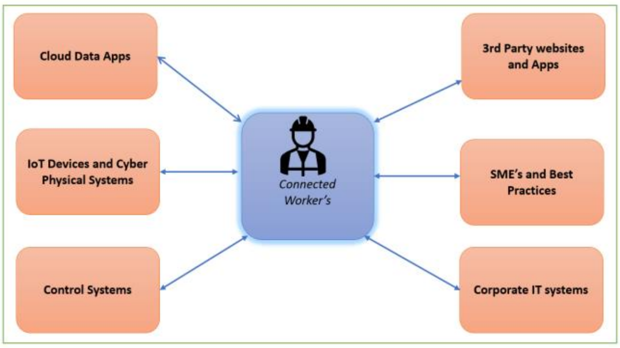


**Fig 7.** Cybersecurity and connected workers at manufacturing facilities

### 4.1 Possible Solutions/ SAP Cloud Services' Zero-Trust Principles Approach

Consider SAP AG's prospective cloud services and apply Zero Trust Architecture concepts without concentrating on setup specifics. To mitigate cybersecurity risk, conduct risk assessments. To protect digital assets against frequent assaults and minimize overall risk, implement well-defined cyber security policies, standards, and guidelines, such as identity and access management, continuous logging, and monitoring. The zero-trust principles' fundamental architectural components are highlighted in the figure that follows. In a hybrid environment, the objective is to safeguard infrastructure, data, business apps, endpoints, and corporate identities, and secure internal and external network connections. Each session has to have trust built and every data flow validated. It is necessary to create a dynamic security policy and deploy enforcement points periodically. The implementation of the least privilege principle, system-to-system API security, authentication and authorization management, privileged credential management, and security automation are all included in this. SAP clients can access the SAP: Zero Trust Architecture documents that the SAP Trust Center has produced. This offers in-depth knowledge of the architectural components.

Business is facilitated by Zero Trust Architecture. It includes an architectural foundation, people, processes, and technology. Nonetheless, there are inherent hazards. Managing those hazards is a multifaceted task. Creating and implementing access controls and enforcing them at different points are necessary to manage this risk to the company. A shift in organizational culture, support from business stakeholders, planning, asset inventory development, complicated data flow mapping, micro-segmenting networks to reduce blast radius, and a comprehensive approach to safeguarding hybrid multi-cloud environments are all needed to achieve such a paradigm shift. To ensure that persons, devices, systems, and processes that interact with corporate data are safe, security controls are necessary. Once they are in place, risks related to the interaction may be efficiently managed. A client may select extra equipment and outside solutions to safeguard their surroundings due to the wide range of options offered. To do this, SAP cloud services provide clients with an extensive toolkit for creating a zero-trust architecture and securing environments that are both SAP and non-SAP [24-25].

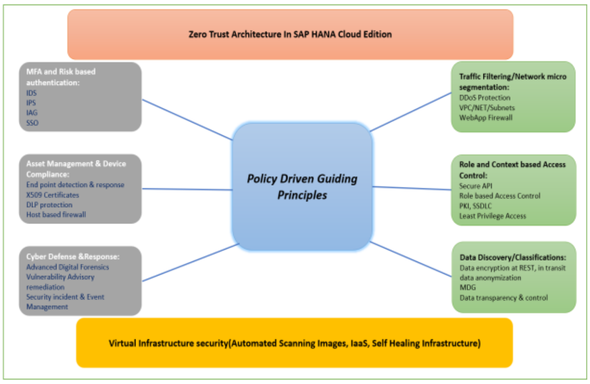
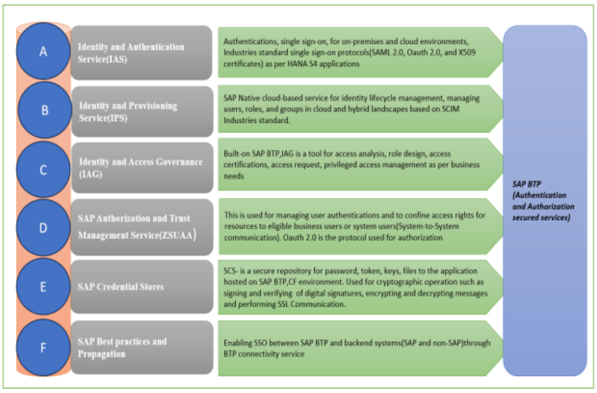

Zero Trust Architecture In SAP HANA Cloud Edition
MFA and Risk based authentication:
IDS
IPS
IAG
SSO
Asset Management & Device Compliance:
End point detection & response
X509 Certificates
DLP protection
Host based firewall
Cyber Defense &Response:
Advanced Digital Forensics
Vulnerability Advisory remediation
Security incident & Event Management
Policy Driven Guiding Principles
Traffic Filtering/Network micro segmentation:
DDoS Protection
VPC/NET/Subnets
WebApp Firewall
Role and Context based Access Control:
Secure API
Role based Access Control
PKI, SSDLC
Least Privilege Access
Data Discovery/Classifications:
Data encryption at REST, in transit
data anonymization
MDG
Data transparency & control
Virtual Infrastructure security(Automated Scanning Images, IaaS, Self Healing Infrastructure)

**Fig. 8.** Zero-trust architecture in SAP HANA Cloud Edition

### 4.2 SAP BTP

SAP uses SAP Cloud Identity Services as a centralized point of authentication in cloud and hybrid environments. SAP Cloud Identity Services is powered by the SAP Business Technology Platform, which includes Identity Provisioning and Identity Authentication Services. Without requiring extra payments, SAP Identity Authentication Services are included in several SAP cloud services packages. Services for SSO, on-premises integration, user management, and authentication are offered by Identity Authentication. User self-services like password resets and employee and partner registration are among the alternatives provided. The Identity Provisioning Service (IPS) manages the secure identity lifecycle for SAP Identity Management, allowing users and groups to be provisioned to and from SCIM systems using the industry standard SCIM2.0 protocol.



| | | |
|---|---|---|
| A | Identity and Authentication Service(IAS) | Authentications, single sign-on, for on-premises and cloud environments, Industries standard single sign-on protocols(SAML 2.0, Oauth 2.0, and X509 certificates) as per HANA S4 applications |
| B | Identity and Provisioning Service(IPS) | SAP Native cloud-based service for identity lifecycle management, managing users, roles, and groups in cloud and hybrid landscapes based on SCIM Industries standard. |
| C | Identity and Access Governance (IAG) | Built-on SAP BTP,IAG is a tool for access analysis, role design, access certifications, access request, privileged access management as per business needs |
| D | SAP Authorization and Trust Management Service(ZSUAA) | This is used for managing user authentications and to confine access rights for resources to eligible business users or system users(System-to-System communication). Oauth 2.0 is the protocol used for authorization |
| E | SAP Credential Stores | SCS- is a secure repository for password, token, keys, files to the application hosted on SAP BTP,CF environment. Used for cryptographic operation such as signing and verifying of digital signatures, encrypting and decrypting messages and performing SSL Communication. |
| F | SAP Best practices and Propagation | Enabling SSO between SAP BTP and backend systems(SAP and non-SAP)through BTP connectivity service |

**Fig 9.** SAP BTP and Interface that supports the prevention of Cybersecurity and Cryptography

### 4.3 Quantum Entanglement in Industrial Manufacturing Sites

Cybersecurity risks are becoming a major worry for both businesses and governments in an increasingly digital environment. The potential real-world uses of quantum entanglement have been proven by researchers at Heriot-Watt's Institute of Photonic and Quantum Sciences. An unbreakable encryption system where data is safely sent between two or more users can be created by utilizing quantum entanglement. It can identify any attempts at illegal access and produce an alert that enables security teams to act promptly and efficiently. A phenomenon known as quantum entanglement occurs when two or more particles, even those that are separated by a great distance, are coupled in such a way that their states cannot be independently described of one another. Particles can exist in a superposition of states in quantum physics, which allows them to exist in several states at once until they are measured. The state of one particle depends on the state of the other when two particles are entangled because of the correlation that develops between their wave functions. This connection, known as entanglement, implies that even in cases when there is a significant distance between two particles, the state of one particle may be instantly identified based on measurements of the other.

The mathematical description of the entangled system, which prevents the wave function of the composite system from being divided into independent wave functions for each particle, helps to explain this occurrence. This implies that independent of the distance between the two particles, a measurement of one will instantaneously collapse their wave functions and reveal their states. Non-local behavior is the result of instantaneous, faster-than-light communication between entangled particles. Entanglement is a fundamental component of quantum technologies, such as quantum computing, quantum teleportation, and quantum cryptography**.** It has been demonstrated by several experiments, including the well-known Einstein-Podolsky-Rosen (EPR) dilemma. In the study of quantum physics, the idea of entanglement is still being explored in depth to fully comprehend its implications and potential uses.

### 4.4 Machine Learning Models In Industrial Espionage

A Generative Adversarial Network (GAN) is a form of artificial neural network that can simulate training data by producing novel data sets with similar structures and distributions. Cyber security-related GAN applications of GANs include the generation of synthetic data for use in training machine learning models to detect cyber threats. A GAN, after being trained on a dataset of real-world traffic, could be used to generate artificial network traffic that closely resembles real-world traffic. A machine learning model could be prepared using this simulated traffic to spot malicious or suspicious activity in real-world networks. A

GAN is then trained using data representing typical internet traffic. A GAN comprises two neural networks: a generator network and a discriminator network. One network, the generator network, is taught to simulate natural-sounding traffic, while another, the discriminator network, learns to tell the difference between authentic and simulated data. The discriminator network uses its available representation of typical network traffic to spot deviations in the new traffic presented to the GAN. With a more extensive and varied dataset available for training, GANs may increase the efficiency of machine learning models used in cyber security. However, GANs can be challenging to develop and fine-tune and need regular attention and updates to function correctly. Ethical issues, such as the potential for misuse or abuse of the technology, can also be raised by including synthetic data in machine learning models.

$$L(y, y) = [y.\log y + (1 - \underset{\uparrow}{y}.\log(1 - \underset{\uparrow}{y})]$$

Original Data Reconstructed data

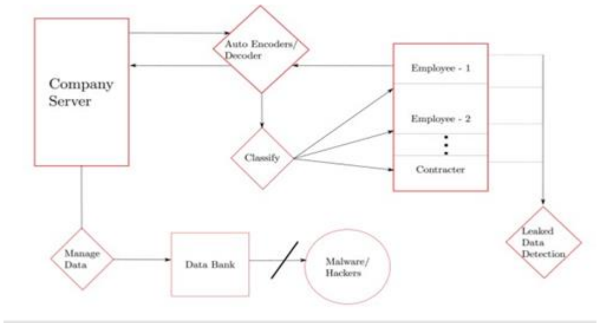


**Fig 10.** Sample flow diagram of auto-encoders to mitigate security threats.

The Generative Adversarial Network is composed of two models: discriminative and generative. The discriminative model compares police trying to seize counterfeit money, whereas the generative model is like a counterfeiter trying to make fake money and spend it covertly. This competition will continue until the counterfeiter gets sophisticated enough to fool the police or any other form of security organization.

Some of the mathematical formula represents the GAN mathematical formula:

*G = Generator*

*D = Discriminator*

*$\Theta_d$= Parameters of discriminators*

*$P_{data}$ (x)= Original data distribution*

*$\Theta_{g\,=}$ Parameters of generator*

*Pz(z)= Input noise distribution*

*$P_g$(x)= Generated distribution*

### 4.4.1 Derivation of the Loss Function

The binary cross-entropy loss formula may be used to generate the loss function given in the original research by Ian Goodfellow et al. The binary cross-entropy loss may be expressed as follows:

### 4.4.2 Discriminator Loss

The label of the data arriving from Pdata (x) for the discriminator's training is y=1 (actual data) and y^ = D(x). We get the above loss function by substituting this.

$$L(D(x).1 = \log(D(x) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1).$$

Additionally, the label for data originating from the generator is y^= D(G(z)) and y= 0 (fake. data).

*So, in this case,* $L(D(G(z)),0 = \log(1 - D(G(z)))$ *……………………. (2).*

### 4.4.3 GNN Deep Learning Model

GNNs are deep learning algorithms that do inference on graph-described data, accomplishing tasks such as node-level, edge-level, and graph-level prediction. In tasks such as picture classification, identification, and object recognition, they outperform Convolutional Neural Networks (CNNs). CNNs detect spatially localized information by employing a set of receptive fields in kernel form and hidden convolution and pooling layers.

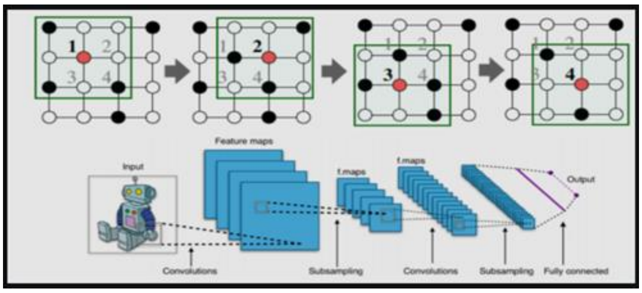


**Fig 11**. CNN on an Images

### 4.5. Types of GNN

There are many forms of graph neural networks, each with a specific function. Gated graph neural networks, recurrent graph neural networks, and graph convolutional networks are a few examples of these.

### 4.5.1 Recurring graph neural network, or RGNN

The Banach Fixed-Point Theorem assumption is the foundation of the RecGNN. Let (X,d) be a full metric space and let (T: X→X) be a contraction mapping by the Banach Fixed-Point Theorem. After that, T has a single fixed point (x∗), and the sequence T_n(x) for all x in X converges to (x∗) for all n.

This indicates that after applying the mapping T to x k times, x^k ought to be almost equivalent to x^(k-1).

$x^k = T\,(x^{k-1}),\ k \in (1,\ n)$

RecGNN defines a parameterized function f_w:

$x_n = f_w\,(l_n\ ,\ l_{\ co[n]}\ ,\ x_{\ ne[n]},\ l_{ne[n]})$

Here l_n, l_co, x_ne, and l_ne represent the features of the current node [n], the edges of the node [n], the state of the neighboring nodes, and the features of the neighboring nodes.

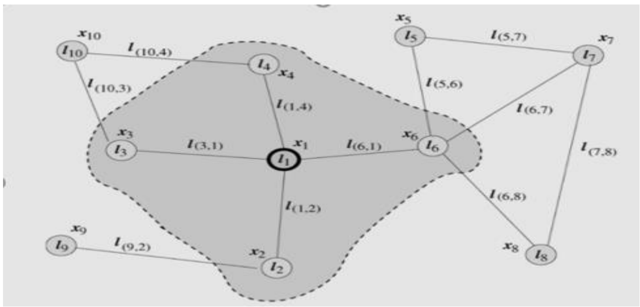


**Fig 12.** CNN on an Images

The node status update seen in the above picture is based on data from its neighbors in the GNN models. To decide each node, the graph neural network model ultimately generates an output depending on the final node state after k repetitions. Here is the output function:

$O_n = g_w\,(x_n,\ l_n)$

$$\chi_1 = \mathbf{f}_{\mathbf{w}}\,(\underbrace{\mathbf{l}_1,\ \mathbf{l}_{(1,2)},\ \mathbf{l}_{(3,1)},\ \mathbf{l}_{(1,4)},\ \mathbf{l}_{(6,1)}}_{l_{co[1]}},\ \underbrace{\mathbf{x}_2,\ \mathbf{x}_3,\ \mathbf{x}_4,\ \mathbf{x}_6}_{x_{ne[1]}},\underbrace{\mathbf{l}_{2,}\mathbf{l}_{3,}\mathbf{l}_{4,}\mathbf{l}_{6,}}_{l_{ne[n]}})$$

### 4.5.2 GCN

Among the GNNs (Graph Convolutional Networks) kinds that are most often used are those. They are comparable to convolutional neural networks in function; therefore, they might be used to picture segmentation and classification. GCN approaches are classified into two categories: spectral graph convolutional networks and spatial graph convolutional networks.

### 4.5.3 Spatial Graph Convolutional Network (SGCN)

Spatial graph convolutional networks combine the features of nearby nodes into the center node, much as convolutional neural networks do. In short, convolution is the sum of adjacent pixels around a center pixel in an image specified by a filter with learnable weight and adjustable size. Using SGCNs, comparable outcomes are achieved with graph-structured data. Spectral graph convolutional networks offer a strong mathematical foundation compared to other GNNs. Graph convolution simplification and approximation, together with graph signal processing theory, serve as the foundation for the spectral convolutional network. The following is the reduction of graph convolution to:

$$g_{\theta 1} * x \ \square \ \sum_{k=0}^{k} \boldsymbol{\theta}_{\ k} T_k\,(\Lambda\,)$$

### 4.5.4 Equations

Number equations consecutively with equation numbers in parentheses flush with the right margin, as in (1). First, use the equation editor to create the equation. Then select the “Equation” markup style. Press the tab key and write the equation number in parentheses. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents. Use parentheses to avoid ambiguities in denominators. Punctuate equations when they are part of a sentence, as in

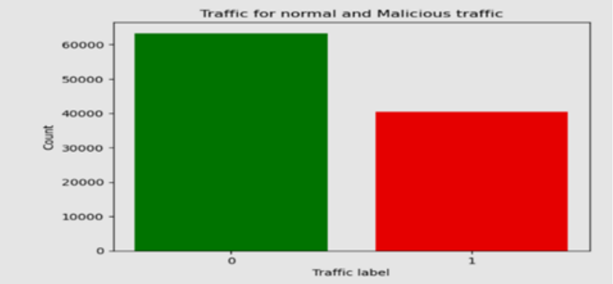


**Fig 13.** Traffic for Normal and Malicious attack

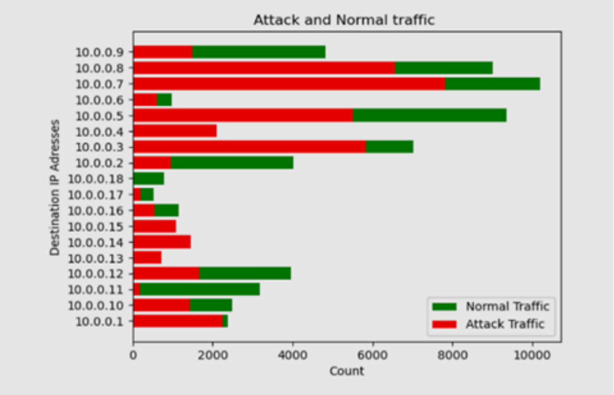


**Fig 14.** Traffic for Normal and Malicious attacks with Destination IP

### 4.6 Preventive and Correct Measure while Considering the Best Practices in Industrial Espionage

The below steps are the best approaches to implement to prevent industrial espionage in manufacturing sites.

- Conduct a risk assessment as per the ISMS Audit log of the GMP.
- Stick to standard operating procedures and company directives.
- Procedures and processes should be documented as a process asset in an organization.
- Verify that SOPs are working as intended.

- Formulate and implement functional systems.
- Keep all infrastructures running smoothly.
- Enhance workers' abilities on the job.
- Maintaining a spotless environment is essential for avoiding the spread of disease.
- Set quality first and incorporate it into existing processes.
- Maintenance of Good Manufacturing Practices Audits
- Secure your infrastructure as required in manufacturing sites.
- Establish an effective security policy.
- Think of your employee’s security-wise and monitor employee activity.
- Manage data access wisely and develop a reliable incident response plan.
- Implement high-end ERP and cloud applications to prevent industrial espionage.

## 5. Conclusion and Future Research

This article examines recent research on Industrial Espionage (IE) and offers a working definition, outlining important aspects, recent findings, and possible directions for further study. The goal is to build multidisciplinary and multi-agency cooperation to establish more morally and practically sound IE countermeasures, including preventative standards and best practices. The study recognizes that IE is a relatively young, multidisciplinary topic with several challenges, such as the need for more research and future study scope.

1. Lack of a common definition: Several terms, including "economic espionage," "commercial intelligence," "competitive intelligence," "industrial espionage," and "cyber espionage," are frequently used synonymously to refer to a wide range of illicit business activities that are relevant to the manufacturing industries.
2. Because research is often carried out in separate academic departments, the scientific community in IE suffers from a lack of collaboration. The absence of a unifying framework prevents critical analysis and building upon each other's discoveries, leaving the field disorganized and unclear for novice researchers.

It is vital to have a precise definition of IE to eliminate any confusion and guide the direction of any potential future studies. To this end, we have first defined Industrial Espionage (IE) and Competitive Intelligence (CI), two controversial but necessary business practices for making this distinction. We then derived a working definition of IE and explained the best way to prevent and protect the critical confidential information of manufacturing sites and production shop-floor information. We have added case studies and better ways to avoid IE in industrial cybercrimes. It's crucial to remember that although AI greatly improves security procedures, it is not infallible. Attackers with advanced skills may try to get around AI-based defenses by using strategies that imitate typical behavior or take advantage of flaws in AI systems. Thus, to effectively counter industrial espionage and other cyber threats, a multi-layered strategy that incorporates.

### Data Availability Statement

The authors declare that all data supporting the findings of this study are available within the article.

### Conflicts of interest

The authors declare no conflicts of interest.

### References

[1] W.-K. Chen, Linear Networks and Systems. Belmont, CA, USA: Wadsworth, 1993, pp. 123–135.

[2] J. U. Duncombe, “Infrared navigation—Part I: An assessment of feasibility,” IEEE Trans. Electron Devices, vol. ED-11, no. 1, pp. 34–39, Jan. 1959, 10.1109/TED.2016.2628402.

[3] [E. P. Wigner, “Theory of traveling-wave optical laser,” Phys. Rev., vol. 134, pp. A635–A646, Dec. 1965.

[4] B. Senapati, J. R. Talburt, Naeem, A., and V. J. R. Batthula, &quot; Transfer Learning Based Models for Food Detection Using ResNet-50,&quot; 2023 IEEE International Conference on Electro Information Technology (eIT), Romeoville, IL, USA, 2023, pp. 224-229, doi: 10.1109/eIT57321.2023.10187288.

[5] Noh, H., S. Hong, and B. Han. Learning deconvolution network for semantic segmentation. in Proceedings of the IEEE international conference on computer vision. 2015.

[6] Naeem, A.B.; Senapati, B.; Islam Sudman, M.S.; Bashir, K.; Ahmed, A.E.M. Intelligent Road Management System for Autonomous, Non-Autonomous, and VIP Vehicles. World Electr. Veh. J. 2023, 14, 238.https://doi.org/10.3390/wevj14090238.

[7] Zhu, L. et al. (2023). Make-A-Volume: Leveraging Latent Diffusion Models for Cross-Modality 3D Brain MRI Synthesis. In: Greenspan, H., et al. Medical Image Computing and Computer-Assisted Intervention – MICCAI 2023. MICCAI 2023. Lecture Notes in Computer Science, vol 14229. Springer, Cham. https://doi.org/10.1007/978-3-031-43999-5_56.

[8] Soomro, A.M.; Naeem, A.B.; Senapati, B.; Bashir, K.; Pradhan, S.; Maaliw, R.R.; Sakr, H.A. Constructor Development: Predicting Object Communication Errors. In Proceedings of the 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&amp; T), Bahawalpur, Pakistan, 9–11 January 2023; pp. 1–7.

[9] Zikic, D., et al., Segmentation of brain tumor tissues with convolutional neural networks. Proceedings MICCAI-BRATS, 2014: p. 36-39.

[10] Naeem, A. B., Soomro, A. M., Saim, H. M., &amp; amp; Malik, H. (2023). Smart Road Management System for prioritized autonomous vehicles under vehicle-to-everything (V2X) communication. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-023-16950-1.

[11] A. B. Naeem et al., "Heart Disease Detection Using Feature Extraction and Artificial Neural Networks: A Sensor-Based Approach," in IEEE Access, vol. 12, pp. 37349-37362, 2024, doi: 10.1109/ACCESS.2024.3373646.

[12] E. E. Reber, R. L. Michell, and C. J. Carter, “Oxygen absorption in the earth’s atmosphere,” Aerospace Corp., Los Angeles, CA, USA, Tech. Rep. TR-0200 (4230-46)-3, Nov. 1988.

[13] J. H. Davis and J. R. Cogdell, “Calibration program for the 16-foot antenna,” Elect. Eng. Res. Lab., Univ. Texas, Austin, TX, USA, Tech. Memo. NGL-006-69-3, Nov. 15, 1987.

[14] Naeem, A. B. ., Senapati, B. ., Mahadin, G. A. ., Ghulaxe, V. ., Almeida, F. ., Sudman, S. I. ., & Ghafoor, M. I. . (2024). Determine the Prevalence of Hepatitis B and C During Pregnancy by Using a Machine Learning Algorithm. International Journal of Intelligent Systems and Applications in Engineering, 12(13s), 744–751. Retrieved from https://www.ijisae.org/index.php/IJISAE/article/view/4704

[15] Transmission Systems for Communications, 3rd ed., Western Electric Co., Winston-Salem, NC, USA, 1985, pp. 44–60.

[16] Motorola Semiconductor Data Manual, Motorola Semiconductor Products Inc., Phoenix, AZ, USA, 1989.

[17] G. O. Young, “Synthetic structure of industrial plastics,” in Plastics, vol. 3, Polymers of Hexadromicon, J. Peters, Ed., 2nd ed. New York, NY, USA: McGraw-Hill, 1964, pp. 15-64. [Online]. Available: http://www.bookref.com.

[18] Senapati, B. et al. (2024). Wrist Crack Classification Using Deep Learning and X-Ray Imaging. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the Second International Conference on Advances in Computing Research (ACR’24). ACR 2024. Lecture Notes in Networks and Systems, vol 956. Springer, Cham. https://doi.org/10.1007/978-3-031-56950-0_6

[19] The Founders’ Constitution, Philip B. Kurland and Ralph Lerner, eds., Chicago, IL, USA: Univ. Chicago Press, 1987. [Online]. Available: http://press-pubs.uchicago.edu/founders/

[20] The Terahertz Wave eBook. ZOmega Terahertz Corp., 2014. [Online]. Available: http://dl.z-thz.com/eBook/zomega_ebook_pdf_1206_sr.pdf. Accessed on: May 19, 2014.

[21] Naeem, Awad Bin, Biswaranjan Senapati, Md. Sakiul Islam Sudman, Kashif Bashir, and Ayman E. M. Ahmed. 2023. "Intelligent Road Management System for Autonomous, Non-Autonomous, and VIP Vehicles" World Electric Vehicle Journal 14, no. 9: 238. https://doi.org/10.3390/wevj14090238.

[22] Philip B. Kurland and Ralph Lerner, eds., The Founders’ Constitution. Chicago, IL, USA: Univ. of Chicago Press, 1987, Accessed on: Feb. 28, 2010, [Online] Available: http://press-pubs.uchicago.edu/founders/

[23] J. S. Turner, “New directions in communications,” IEEE J. Sel. Areas Commun., vol. 13, no. 1, pp. 11-23, Jan. 1995.

[24] W. P. Risk, G. S. Kino, and H. J. Shaw, “Fiber-optic frequency shifter using a surface acoustic wave incident at an oblique angle,” Opt. Lett., vol. 11, no. 2, pp. 115–117, Feb. 1986.

[25] P. Kopyt et al., “Electric properties of graphene-based conductive layers from DC up to terahertz range,” IEEE THz Sci. Technol., to be published. DOI: 10.1109/TTHZ.2016.2544142.